Política de Certificado Multicert

Políticas

MULTICERT_PJ.ECRAIZ_426_pt

Identificação da EC: PKI

Nível de Acesso: Público

Versão: 10.0

Data: 01/07/2023

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Rua Carlos Pinto Coelho, 13, 2720-092 Amadora
Telefone: +351 217 123 010

Identificação de Documento: MULTICERT_PJ.ECRAIZ_426_pt

Palavras-chave:

Tipo de Documento: Políticas

Título: Política de Certificado Multicert

Língua Original: Português

Língua de Publicação: Português

Nivel de Acesso: Público

Data: 01/07/2023

Versão Atual: 10.0

Identificação da EC: PKI

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	29/05/2018	Revisão de acordo com RFC 3647 e Baseline Requirements 1.5.7 do CABForum	Multicert S.A.
1.1-1.4	25/09/2018	Inclusão de procedimento para método de prova de controlo do endereço de email. Inclusão de práticas para re-key, inclusão de declaração sobre EC`s externas	Multicert S.A.
2.0	01/10/2018	Aprovação	Multicert S.A.
2.1	29/01/2019	Revisão de razões de revogação	Multicert S.A.
3.0	29/01/2019	Aprovação	Multicert S.A.
3.1	25/03/2019	Revisão de acordo com Baseline Requirements v1.6.4	Multicert S.A.
4.0	25/03/2019	Aprovação	Multicert S.A.
4.1	25/03/2019	Inclusão de informação sobre PSD2	Multicert, S.A.
5.0	09/12/2019	Aprovação	Multicert, S.A.
5.1	10/12/2020	Revisão de acordo com DPC v10	Multicert S.A.
6.0	17/12/2020	Aprovação	Multicert S.A.
6.1	29/10/2021	Revisão geral da secção 5 | Atualização de secção 3.2.2.2 métodos de validação de domínio/IP	Multicert S.A.
7.0	31/03/2022	Aprovação	Multicert S.A.
7.1	15/09/2022	Revisão secção 4.8	Multicert S.A.
8.0	02/11/2022	Aprovação	Multicert S.A.
8.1	06/01/2023	Revisão secção 5	Multicert S.A.
9.0	14/01/2023	Aprovação	Multicert S.A.
9.1	30/06/2023	Remoção certificados SSL OV e WC, atualização de contactos	Multicert S.A.
10.0	01/07/2023	Aprovação	Multicert S.A.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_427_pt	Declaração de Práticas de Certificação	Multicert S.A
MULTICERT_PJ.ECRAIZ_428_pt	Lista de Perfis de Certificados	Multicert S.A.
MULTICERT_PJ.ECRAIZ_621_en	List of Approved Incorporating Agencies	Multicert S.A.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Sumário

Política de Certificado Multicert ... 1
Sumário ... 4
1 Introdução ... 11
1.1 Visão Geral ... 11
1.2 Nome e Identificação do Documento ... 11
1.3 Participantes PKI ... 13
1.3.1 Entidades de Certificação ... 13
1.3.1.1 Entidades de Certificação Externas ... 13
1.3.2 Entidades de Registo ... 14
1.3.3 Subscritores / Titulares ... 14
1.3.4 *Relying Parties* ... 14
1.3.5 Outros Participantes ... 14
1.4 Utilização do Certificado ... 14
1.4.1 Utilizações Apropriadas de Certificado ... 15
1.4.2 Utilizações Proibidas de Certificado ... 15
1.5 Gestão da Política ... 15
1.5.1 Entidade Responsável pela Gestão do Documento ... 15
1.5.2 Contacto ... 15
1.5.3 Responsável por Determinar a Conformidade da PC ... 16
1.5.4 Procedimentos para Aprovação da PC ... 16
1.6 Definições e Acrónimos ... 16
1.6.1 Definições ... 16
1.6.2 Acrónimos ... 21
1.6.3 Referências Bibliográficas ... 23
2 Responsabilidade de Publicação e Repositório ... 25
2.1 Repositórios ... 25
2.2 Publicação de Informação de Certificado ... 25
2.3 Periodicidade de Publicação ... 25
2.4 Controlo de Acesso aos Repositórios ... 25
3 Identificação e Autenticação ... 26
3.1 Atribuição de Nomes ... 26
3.1.1 Tipos de Nomes ... 26
3.1.2 Necessidade de Nomes Significativos ... 26
3.1.3 Anonimato ou Pseudónimo de Subscritores/Titulares ... 26
3.1.4 Regras para Interpretação de Formato de Nomes ... 26
3.1.5 Unicidade de Nomes ... 26
3.1.6 Reconhecimento, Autenticação, e Função de Marcas Registadas ... 27
3.2 Validação de Identidade Inicial ... 27
3.2.1 Método de Prova de Posse da Chave Privada ... 27
3.2.2 Autenticação de Identidade da Organização ... 27

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

3.2.2.1 Método de Prova de Controlo de Endereço de Email ... 27
3.2.2.2 Método de Validação de Controlo de Nome de Domínio / Endereço IP ... 27
3.2.3 Autenticação de Identidade do Indivíduo ... 27
3.2.4 Informação do Subscritor/Titular Não Verificada ... 28
3.2.5 Validação de Autoridade ... 28
3.2.6 Critérios para Interoperabilidade ... 28
3.3 Identificação e Autenticação para Pedidos de *Re-Key* ... 28
3.3.1 Identificação e Autenticação para Pedidos de Rotina de *Re-Key* ... 28
3.3.2 Identificação e Autenticação para *Re-Key* após Revogação ... 28
3.4 Identificação e Autenticação para Pedido de Revogação ... 28
4 Requisitos Operacionais do Ciclo de Vida do Certificado ... 29
4.1 Pedido de Certificado ... 29
4.1.1 Quem Pode Submeter um Pedido de Certificado ... 29
4.1.2 Processo de Registo e Responsabilidades ... 29
4.2 Processamento do Pedido de Certificado ... 29
4.2.1 Desempenhando Funções de Identificação e Autenticação ... 29
4.2.2 Aprovação ou Rejeição de Pedidos de Certificado ... 29
4.2.3 Prazo de Processamento de Pedidos de Certificado ... 29
4.3 Emissão de Certificado ... 30
4.3.1 Ações da EC durante a Emissão do Certificado ... 30
4.3.2 Notificação ao Subscritor/Titular pela EC Emissora do Certificado ... 30
4.4 Aceitação do Certificado ... 30
4.4.1 Conduta que Constitui a Aceitação do Certificado ... 30
4.4.2 Publicação do Certificado pela EC ... 30
4.4.3 Notificação da Emissão do Certificado pela EC a Outras Entidades ... 30
4.5 Utilização do Certificado e Par de Chaves ... 30
4.5.1 Utilização do Certificado e Par de Chaves pelo Subscritor/Titular ... 30
4.5.2 Utilização do Certificado e Chave Pública pela *Relying Party* ... 31
4.6 Renovação de Certificado ... 31
4.6.1 Circunstâncias para a Renovação do Certificado ... 31
4.6.2 Quem Pode Solicitar a Renovação ... 31
4.6.3 Processamento de Pedidos de Renovação de Certificado ... 31
4.6.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular ... 31
4.6.5 Conduta que Constitui a Aceitação do Certificado Renovado ... 32
4.6.6 Publicação do Certificado Renovado pela EC ... 32
4.6.7 Notificação do Certificado Emitido pela EC a Outras Entidades ... 32
4.7 *Re-Key* de Certificado ... 32
4.7.1 Circunstâncias para *Re-Key* de Certificado ... 32
4.7.2 Quem Pode Solicitar a Certificação de uma Nova Chave Pública ... 32
4.7.3 Processamento de Pedidos de *Re-Key* de Certificado ... 32
4.7.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular ... 33
4.7.5 Conduta que Constitui a Aceitação do Certificado para o qual foi feito *Re-Key* ... 33
4.7.6 Publicação do Certificado pela EC para o qual foi feito *Re-Key* ... 33
4.7.7 Notificação de Emissão de Certificado pela EC a Outras Entidades ... 33
4.8 Modificação de Certificado ... 33

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.8.1 Circunstâncias para a Modificação de Certificado ... 33
4.8.2 Quem Pode Solicitar a Modificação de Certificado ... 33
4.8.3 Processamento de Pedidos de Modificação de Certificado ... 33
4.8.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular ... 34
4.8.5 Conduta que Constitui Aceitação de Certificado Modificado ... 34
4.8.6 Publicação do Certificado Modificado pela EC ... 34
4.8.7 Notificação de Emissão de Certificado pela EC a Outras Entidades ... 34
4.9 Revogação e Suspensão de Certificado ... 34
4.9.1 Motivos para Revogação ... 34
4.9.2 Quem Pode Solicitar Revogação ... 36
4.9.3 Procedimento para o Pedido de Revogação ... 36
4.9.4 Período de Carência do Pedido de Revogação ... 36
4.9.5 Tempo de Processamento do Pedido de Revogação pela EC ... 36
4.9.6 Requisito de Verificação da Revogação pelas *Relying Parties* ... 36
4.9.7 Frequência de Emissão de CRL ... 37
4.9.8 Latência Máxima para CRLs ... 37
4.9.9 Disponibilidade de Verificação de Estado/Revogação *On-Line* ... 37
4.9.10 Requisitos de Verificação de Revogação *On-Line* ... 37
4.9.11 Outras Formas Disponíveis de Anunciar Revogação ... 37
4.9.12 Requisitos Especiais Relacionados com o Comprometimento de Chave ... 37
4.9.13 Motivos para a Suspensão ... 38
4.9.14 Quem Pode Solicitar Suspensão ... 38
4.9.15 Procedimento para o Pedido de Suspensão ... 38
4.9.16 Limites do Período de Suspensão ... 38
4.10 Serviços de Estado de Certificado ... 38
4.10.1 Características Operacionais ... 38
4.10.2 Disponibilidade de Serviço ... 38
4.10.3 Funcionalidades Opcionais ... 38
4.11 Fim de Subscrição ... 38
4.12 Custódia e Recuperação de Chaves ... 39
4.12.1 Política e Práticas de Custódia e Recuperação de Chaves ... 39
4.12.2 Política e Práticas de Encapsulamento e Recuperação de Chave de Sessão ... 39
5 Controlos de Segurança Física, Gestão e Operacionais ... 40
5.1 Controlos de Segurança Física ... 40
5.1.1 Localização Física e Tipo de Construção ... 40
5.1.2 Acesso Físico ... 41
5.1.3 Energia e Ar Condicionado ... 41
5.1.4 Exposição à Água ... 42
5.1.5 Prevenção e Proteção contra Incêndio ... 42
5.1.6 Armazenamento de *Media* ... 42
5.1.7 Eliminação de Resíduos ... 42
5.1.8 *Backup* em Instalações Externas ... 43
5.2 Controlos Procedimentais ... 43
5.2.1 Grupos de Trabalho ... 43
5.2.1.1 Grupo de Trabalho de Operação ... 43

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.2.1.2 Grupo de Trabalho de Autenticação ... 44
5.2.1.3 Grupo de Trabalho de Auditoria ... 44
5.2.1.4 Grupo de Trabalho de Custódia ... 44
5.2.1.5 Grupo de Trabalho de Operação de Registo ... 44
5.2.1.6 Grupo de Trabalho de Administração de Sistemas ... 44
5.2.1.7 Grupo de Trabalho de Gestão ... 44
5.2.1.8 Grupo de Trabalho de Manutenção ... 44
5.2.2 Número de Pessoas Exigidas por Tarefa ... 45
5.2.3 Identificação e Autenticação por Função ... 45
5.2.4 Funções que Requerem Separação de Responsabilidades ... 45
5.3 Controlos de Segurança Pessoal ... 46
5.3.1 Requisitos relativos a Qualificações, Experiência, e Autorização ... 46
5.3.2 Procedimentos de Verificação de Antecedentes ... 46
5.3.3 Requisitos de Formação ... 46
5.3.4 Frequência e Requisitos para Atualização de Formação ... 47
5.3.5 Frequência e Sequência da Rotação de Funções ... 47
5.3.6 Sanções para Ações Não Autorizadas ... 47
5.3.7 Requisitos para Prestadores de Serviços Independentes ... 47
5.3.8 Documentação Fornecida ao Pessoal ... 47
5.4 Procedimentos de Registo de Auditoria ... 48
5.4.1 Tipos de Eventos Registados ... 48
5.4.2 Frequência de Processamento de Registos ... 48
5.4.3 Período de Retenção de Registos de Auditoria ... 48
5.4.4 Proteção de Registos de Auditoria ... 48
5.4.5 Procedimentos de Cópia de Segurança de Registos de Auditoria ... 48
5.4.6 Sistema de Recolha de Registos (Interno vs. Externo) ... 49
5.4.7 Notificação de Agentes Causadores de Eventos ... 49
5.4.8 Avaliações de Vulnerabilidades ... 49
5.5 Arquivo de Registos ... 49
5.5.1 Tipos de Registos Arquivados ... 49
5.5.2 Período de Retenção em Arquivo ... 49
5.5.3 Proteção do Arquivo ... 49
5.5.4 Procedimentos para Cópia de Segurança do Arquivo ... 49
5.5.5 Requisitos para Validação Cronológica de Registos ... 50
5.5.6 Sistema de Recolha de Arquivo (Interno ou Externo) ... 50
5.5.7 Procedimentos para Obter e Verificar Informação de Arquivo ... 50
5.6 Renovação de Chaves ... 50
5.7 Recuperação em Caso de Desastre ou Comprometimento ... 50
5.7.1 Procedimentos em Caso de Incidente ou Desastre ... 50
5.7.2 Recursos Computacionais, Software e/ou Dados Corrompidos ... 50
5.7.3 Procedimentos em caso de Comprometimento de Chave Privada da Entidade ... 51
5.7.4 Capacidades de Continuidade de Negócio em caso de Desastre ... 51
5.8 Cessação da EC ou ER ... 51
6 Controlos de Segurança Técnica ... 52
6.1 Geração e Instalação do Par de Chaves ... 52

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

6.1.1 Geração do Par de Chaves ... 52
6.1.2 Entrega da Chave Privada ao Subscritor/Titular ... 52
6.1.3 Entrega da Chave Pública ao Emissor do Certificado ... 52
6.1.4 Entrega da Chave Pública da EC às *Relying Parties* ... 53
6.1.5 Tamanhos de Chave ... 53
6.1.6 Geração dos Parâmetros de Chave Pública e Verificação de Qualidade ... 53
6.1.7 Finalidades de Utilização da Chave (de acordo com o campo *key usage* X.509 v3) 53
6.2 Proteção de Chave Privada e Controlos de Engenharia de Módulo Criptográfico ... 53
6.2.1 Controlos e *Standards* de Módulo Criptográfico ... 53
6.2.2 Controlo Multi-Pessoal (n de m) da Chave Privada ... 53
6.2.3 Custódia de Chave Privada ... 54
6.2.4 Cópia de Segurança da Chave Privada ... 54
6.2.5 Arquivo de Chave Privada ... 54
6.2.6 Transferência da Chave Privada para/de um Módulo Criptográfico ... 54
6.2.7 Armazenamento da Chave Privada em Módulo Criptográfico ... 55
6.2.8 Método de Ativação da Chave Privada ... 55
6.2.9 Método de Desativação da Chave Privada ... 55
6.2.10 Método de Destruição da Chave Privada ... 55
6.2.11 Avaliação/Nível do Módulo Criptográfico ... 55
6.3 Outros Aspetos da Gestão do Par de Chaves ... 55
6.3.1 Arquivo da Chave Pública ... 55
6.3.2 Períodos Operacionais do Certificado e Períodos de Utilização do Par de Chaves 56
6.4 Dados de Ativação ... 56
6.4.1 Geração e Instalação de Dados de Ativação ... 56
6.4.2 Proteção de Dados de Ativação ... 56
6.4.3 Outros Aspetos dos Dados de Ativação ... 56
6.5 Controlos de Segurança Computacional ... 56
6.5.1 Requisitos Técnicos Específicos de Segurança Computacional ... 56
6.5.2 Avaliação/Nível de Segurança Computacional ... 57
6.6 Controlos Técnicos do Ciclo de Vida ... 57
6.6.1 Controlos de Desenvolvimento de Sistema ... 57
6.6.2 Controlos de Gestão da Segurança ... 57
6.6.3 Controlos de Segurança do Ciclo de Vida ... 57
6.7 Controlos de Segurança da Rede ... 57
6.8 Validação Cronológica ... 57
7 Perfis de Certificado, CRL e OCSP ... 58
7.1 Perfil de Certificado ... 58
7.1.1 Número(s) de Versão ... 58
7.1.2 Extensões dos Certificados ... 59
7.1.3 Identificadores de Objeto de Algoritmo ... 59
7.1.4 Formatos de Nome ... 59
7.1.5 Restrições de Nome ... 59
7.1.6 Identificador de Objeto de Política de Certificado ... 59

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

7.1.7 Utilização de Extensão de Restrições de Política ... 59
7.1.8 Sintaxe e Semânticas de Qualificadores de Política ... 59
7.1.9 Processamento de Semânticas para a Extensão de Políticas de Certificado Críticas 59
7.2 Perfil de CRL ... 60
7.2.1 Número(s) de Versão ... 60
7.2.2 CRL e Extensões da CRL ... 60
7.3 Perfil OCSP ... 60
7.3.1 Número(s) de Versão ... 60
7.3.2 Extensões OCSP ... 61
8 Auditoria de Conformidade e Outras Avaliações ... 62
8.1 Frequência ou Circunstâncias da Avaliação ... 62
8.2 Identificação/Qualificações do Avaliador ... 62
8.3 Relação do Avaliador com a Entidade Avaliada ... 62
8.4 Tópicos Abrangidos pela Avaliação ... 62
8.5 Ações Tomadas como Resultado de Deficiências ... 63
8.6 Comunicação de Resultados ... 63
9 Outras Matérias Legais e de Negócio ... 64
9.1 Taxas ... 64
9.1.1 Taxas de Emissão ou Renovação de Certificado ... 64
9.1.2 Taxas de Acesso a Certificado ... 64
9.1.3 Taxas de Acesso a Informação de Estado ou Revogação ... 64
9.1.4 Taxas para Outros Serviços ... 64
9.1.5 Política de Reembolso ... 64
9.2 Responsabilidade Financeira ... 64
9.2.1 Cobertura de Seguro ... 64
9.2.2 Outros Recursos ... 64
9.2.3 Cobertura de Seguro ou Garantia para Utilizadores Finais ... 64
9.3 Confidencialidade de Informação de Negócio ... 65
9.3.1 Âmbito de Informação Confidencial ... 65
9.3.2 Informação fora do Âmbito de Informação Confidencial ... 65
9.3.3 Responsabilidade de Proteção de Informação Confidencial ... 66
9.4 Privacidade de Informação Pessoal ... 66
9.4.1 Plano de Privacidade ... 66
9.4.2 Informação Tratada como Privada ... 66
9.4.3 Informação Não Considerada Privada ... 66
9.4.4 Responsabilidade pela Proteção de Informação Privada ... 66
9.4.5 Notificação e Consentimento para Utilização de Informação Privada ... 66
9.4.6 Divulgação Resultante de Processo Judicial ou Administrativo ... 66
9.4.7 Outras Circunstâncias de Divulgação de Informação ... 66
9.5 Direitos de Propriedade Intelectual ... 67
9.6 Representações e Garantias ... 67
9.6.1 Representações e Garantias da EC ... 67
9.6.2 Representações e Garantias da ER ... 68
9.6.3 Representações e Garantias do Subscritor/Titular ... 68

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.6.4 Representações e Garantias das *Relying Party* ... 69
9.6.5 Representações e Garantias de outros Participantes ... 69
9.7 Renúncia de Garantias ... 69
9.8 Limitações de Responsabilidade ... 70
9.9 Indemnizações ... 70
9.10 Prazo e Terminação ... 70
9.10.1 Prazo ... 70
9.10.2 Terminação ... 71
9.10.3 Efeito da Terminação e Sobrevivência ... 71
9.11 Notificações Individuais e Comunicações aos Participantes ... 71
9.12 Alterações ... 71
9.12.1 Procedimento para Alteração ... 71
9.12.2 Mecanismo e Período de Notificação ... 71
9.12.3 Circunstâncias nas quais o OID deve ser Alterado ... 71
9.13 Disposição de Resolução de Conflito ... 72
9.14 Legislação Aplicável ... 72
9.15 Conformidade com a Legislação Aplicável ... 72
9.16 Outras Disposições ... 72
9.16.1 Acordo Completo ... 72
9.16.2 Atribuição ... 72
9.16.3 Divisibilidade ... 72
9.16.4 Execução (Honorários de Advogados e Renúncia de Direitos) ... 73
9.16.5 Força Maior ... 73
9.17 Outras Provisões ... 73
Aprovação ... 74

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

1 Introdução

1.1 Visão Geral

Este documento tem como objetivo definir os requisitos técnicos, organizacionais e procedimentais aplicáveis aos certificados digitais emitidos pelas Entidades de Certificação (EC`s) da Multicert.

Este documento é gerido pelo Grupo de Trabalho de Autenticação e adota a regulamentação e normas listadas na secção 1.6.3. A PKI Multicert está em conformidade com a versão atual das *Baseline Requirements* de acordo com o publicado pelo CA/Browser Forum no documento "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*" disponível em https://www.cabforum.org, seguindo a versão identificada na secção 1.6.3 deste documento. Em caso de discrepância entre este documento e o descrito no documento de *Baseline Requirements*, o que está estabelecido no documento publicado pelo CA/Browser Forum sobrepõe-se ao que está descrito neste documento.

1.2 Nome e Identificação do Documento

Este documento é uma Política de Certificado (PC). A PC é representada no certificado por um número único intitulado "identificador de objeto" (OID).

Este documento é identificado pelos dados incluídos na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 10.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.0.1
Data de Emissão	01/07/2023
Validade	1 Ano
Localização	https://pki.multicert.com/

De forma a uniformizar a informação correspondente à PKI Multicert, esta PC, passa a incorporar as PC`s até então geridas e disponibilizadas por tipo de certificado. Neste sentido, os OID`s correspondentes a cada uma destas PC`s são descontinuados, mas permanecem válidos durante o ciclo de vida dos certificados já emitidos durante a sua vigência. Os seguintes OID`s são descontinuados, mas as informações estão agora presentes neste documento:

- 1.3.6.1.4.1.25070.1.1.1.0.1.1: PC da Multicert Root Certification Authority 01;
- 1.3.6.1.4.1.25070.1.1.1.1.0.1.2: PC para Certificados Qualificados de Assinatura e Selos Eletrónicos Qualificados;
- 1.3.6.1.4.1.25070.1.1.1.1.0.1.3: PC para Certificados de Autenticação;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

- 1.3.6.1.4.1.25070.1.1.1.1.0.1.5: PC para Certificados SSL;
- 1.3.6.1.4.1.25070.1.1.1.2.0.1.1: PC de Validação Cronológica.

A PKI Multicert emite certificados com os seguintes OID's:

Tipo de Certificado	OID Multicert
Assinatura Digital Qualificada	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Assinatura Digital Qualificada para Fatura Eletrónica	1.3.6.1.4.1.25070.1.1.1.1.0.1.22
Selo Eletrónico Qualificado	1.3.6.1.4.1.25070.1.1.1.1.0.1.14
Selo Eletrónico Qualificado para Fatura Eletrónica	1.3.6.1.4.1.25070.1.1.1.1.0.1.19
Selo Eletrónico Qualificado PSD2	1.3.6.1.4.1.25070.1.1.1.1.0.1.14 (até 18/10/2019) 1.3.6.1.4.1.25070.1.1.1.1.0.1.18 (após 18/10/2019)
Autenticação	1.3.6.1.4.1.25070.1.1.1.1.0.1.3
Assinatura Digital Avançada	1.3.6.1.4.1.25070.1.1.1.1.0.1.4
Certificado de Autenticação para Website Qualificado	1.3.6.1.4.1.25070.1.1.1.1.0.1.15
Certificado de Autenticação para Website Qualificado PSD2	1.3.6.1.4.1.25070.1.1.1.1.0.1.12

Para além do OID Multicert, os seguintes certificados estão em conformidade com as seguintes Políticas de Certificados normativas:

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Tipo de Certificado	Identificador de Objeto (OID)	Descrição
Assinatura Digital Qualificada	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
Selo Eletrónico Qualificado	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
Selo Eletrónico Qualificado PSD2	0.4.0.194112.1.1	QCP-l: certificate policy for EU qualified certificates issued to legal persons
Certificado de Autenticação de Website Qualificado e Certificado de Autenticação de Website Qualificado PSD2	0.4.0.194112.1.4	QEVCP-w: certificate policy for EU qualified website authentication certificates based on EVCP
Certificado de Validação Cronológica	0.4.0.2023.1.1	BTSP: a best practices policy for time-stamp

1.3 Participantes PKI

1.3.1 Entidades de Certificação

Todas as EC`s públicas geridas pela Multicert estão credenciadas pelo Gabinete Nacional de Segurança (https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/PT/5), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitadas legalmente a emitir certificados digitais, incluindo certificados digitais qualificados (certificados digitais com o mais elevado grau de segurança previsto na legislação).

Esta política garante que todas as Entidades de Certificação públicas da Multicert devem cumprir com todos os requisitos listados aqui.

A Multicert gere também uma Entidade de Certificação Timestamping (TSA) que fornece prova de data num determinado momento. As condições específicas da TSA encontram-se descritas no documento Declaração de Práticas de Validação Cronológica (MULTICERT_PJ.CA3_24.1.1_0002_pt) disponível em https://pki.multicert.com.

1.3.1.1 Entidades de Certificação Externas

A definição de políticas e dados para a emissão e gestão de certificados para EC`s Subordinadas Externas estão descritas na Política de EC Subordinada, disponível em https://pki.multicert.com.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

1.3.2 Entidades de Registo

As Entidades de Registo (ER) são responsáveis pela identificação dos Subscritores/Titulares dentro de uma organização ou associação e pela validação dos dados necessários à emissão do certificado digital.

As ER`s da Multicert devem assinar um acordo com a EC Multicert, com a finalidade de cumprir todos os requisitos de identificação. É estabelecido um processo e os Operadores de Registo são devidamente identificados e comprometidos com sua Descrição de Função.

1.3.3 Subscritores / Titulares

No contexto deste documento, o termo Subscritor / Titular aplica-se a todos os utilizadores finais para os quais foram atribuídos certificados pela EC Multicert.

São considerados Subscritores / Titulares de certificados emitidos pela EC Multicert aqueles cujo nome está inscrito no campo “Assunto” (*Subject*) do certificado e utilizam o certificado e chave privada correspondente de acordo com o estabelecido neste documento e respetiva Declaração de Práticas de Certificação (DPC), sendo emitidos certificados para as seguintes categorias:

- Pessoa física ou jurídica;
- Pessoa Coletiva (Organizações);
- Serviços (como computadores, firewall, routers, servidores).

1.3.4 *Relying Parties*

As *Relying parties* são pessoas naturais, entidades ou equipamento que atuam com base num certificado e/ou assinatura digital emitido pela EC Emissora.

As *Relying Parties* têm que verificar a CRL ou resposta OCSP adequada antes de confiar na informação constate no certificado.

1.3.5 Outros Participantes

Outros participantes incluem-se todas as Entidades que de alguma forma participam na atividade da EC.

1.4 Utilização do Certificado

Os certificados emitidos no domínio da EC Multicert podem ser utilizados por diferentes Subscritores, sistemas, aplicações, mecanismos e protocolos com o propósito de assegurar os seguintes serviços de segurança:

a) Controlo de Acessos/Autenticação;
b) Confidencialidade;
c) Integridade;
d) Autenticidade; e
e) Não-repúdio.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

1.4.1 Utilizações Apropriadas de Certificado

Os certificados emitidos de acordo com esta PC podem ser usados para controlo de acessos/autenticação, confidencialidade, integridade, autenticidade ou não-repúdio, dependendo da utilização de chave e utilização estendida de chave existentes no certificado.

As utilizações apropriadas de cada tipo de certificado encontram-se definidas na DPC. Os certificados emitidos pela PKI Multicert também são usados pelas Partes de Confiança para a verificação da cadeia de confiança do certificado emitido pela EC Multicert, bem como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida no certificado emitido pelas EC`s da PKI Multicert.

1.4.2 Utilizações Proibidas de Certificado

Os certificados podem ser usados em outros contextos apenas na medida do permitido pela legislação aplicável e não em conflito com a DPC.

1.5 Gestão da Política

1.5.1 Entidade Responsável pela Gestão do Documento

Esta PC e todos os documentos públicos pertencentes à PKI Multicert são geridos pelo Grupo de Trabalho de Autenticação, cujos contactos se encontram indicados na secção 1.5.2.

1.5.2 Contacto

NOME	Grupo de Trabalho de Autenticação da PKI Multicert
Morada:	A/C: Grupo de Trabalho de Autenticação Multicert – Serviços de Certificação Electrónica, S.A. Rua Carlos Pinto Coelho, 13 2720-092 Amadora, Portugal
Correio Eletrónico:	ca.forum@multicert.com Para certificados PSD2: psd2@multicert.com
Página Web:	https://www.multicert.com
Telefone:	+351 217 123 010

No âmbito dos certificados PSD2, caso a NCA pretenda notificar ou comunicar com o TSP, por exemplo, a respeito da comunicação de alterações às informações regulatórias relevantes para o PSD2, ou caso pretenda ser notificada sempre que um certificado PSD2 é emitido ou revogado, ou caso pretenda solicitar a revogação de certificados PSD2 emitidos para um PSP, a NCA deve usar o correio eletrónico acima referido para comunicações relativamente a certificados PSD2.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Os Subscritores, *Relying Parties*, Fornecedores de Aplicações de Software, e outras terceiras partes podem reportar a suspeita de comprometimento da chave privada, uso indevido do certificado, ou outros tipos de fraude, comprometimento, uso indevido, conduta inadequada, ou qualquer outro assunto relacionado com os certificados através do envio de email para os contactos acima.

1.5.3 Responsável por Determinar a Conformidade da PC

O Grupo de Trabalho de Autenticação determina a adequação desta PC e é responsável por verificar a conformidade da DPC com esta PC.

1.5.4 Procedimentos para Aprovação da PC

O Grupo de Trabalho de Gestão é responsável pela aprovação desta política.

1.6 Definições e Acrónimos

1.6.1 Definições

Item	Definição
Acreditação/Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o cumprimento dos requisitos definidos neste documento para os fins nele previstos.
Autoridade de Acreditação/Entidade de Credenciação	Entidade competente para a credenciação e supervisão de entidades certificadoras.
Entidade de Certificação (EC)	Entidade em que um ou mais usuários confia para criar e atribuir certificados. Uma EC pode ser: i) um provedor de serviços de confiança que cria e atribui certificados de chave pública; ou ii) um serviço de geração de certificado técnico que é usado por um provedor de serviços de certificação que cria e atribui certificados de chave pública.
Política de Certificado (PC)	Conjunto denominado de regras que indica a aplicabilidade de um certificado a uma determinada comunidade e/ou classe de aplicativo com requisitos de segurança comuns.
Declaração de Práticas de Certificação (DPC)	Declaração de práticas que uma Entidade de Certificação aplica para a emissão, gestão, revogação, e renovação ou *re-key* de certificados.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Lista de Revogação de Certificados (CRL)	Lista assinada que indica os certificados que foram revogados por um emissor de certificado.
Conformity Assessment Body (CAB)	Significa uma entidade definida pelo ponto 13 do Artigo 2 do Regulamento nº 765/2008, que é acreditada de acordo com esse Regulamento como sendo competente para realizar avaliações de conformidade de um prestador de serviços de confiança qualificado e os serviços de confiança que o prestador presta.
Certificado Digital	Documento eletrónico que associa os dados de verificação de uma assinatura com o seu titular/subscritor e confirma a identidade de tal titular/subscritor.
Assinatura Digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Documento Eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos.
Assinatura Eletrónica	Resultado de um processamento eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Produto de Assinatura Eletrónica	Suporte lógico, dispositivo de equipamento ou seus componentes específicos, destinados a ser utilizados na

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

	prestação de serviços de assinatura eletrónica qualificada por uma entidade certificadora ou na criação e verificação de assinatura eletrónica qualificada.
Certificado Avançado	Certificado que oferece a mesma qualidade de um certificado qualificado, no entanto sem os constrangimentos legais implícitos na assinatura qualificada e sem requisito de utilização de um dispositivo seguro para a sua criação. Não confere o valor probatório legal de uma assinatura qualificada.
Selo Eletrónico Avançado	Um selo eletrónico que obedeça aos requisitos estabelecidos no artigo 36.º do Regulamento (EU) nº 910/2014 do Parlamento Europeu e do Conselho.
Assinatura Eletrónica Avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
OCSP *Responder*	Servidor *online* operado sob a autoridade da EC e conectado ao seu repositório para processar pedidos de estado de certificado.
Online Certificate Status Protocol (OCSP)	Um protocolo *online* de verificação de certificado que permite a aplicações de software de *relying parties* determinar o estado de um certificado identificado.
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Certificado PSD2	Um certificado qualificado que inclui atributos específicos PSD2.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Infraestrutura de Chaves Públicas (ICP ou PKI)	Conjunto de hardware, software, pessoas, procedimentos, regras, políticas e obrigações utilizadas para facilitar de forma confiável a criação, emissão, gestão, e utilização de certificados e chaves baseadas em criptografia de chave pública.
Certificado Qualificado	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I, II III e IV do Regulamento (EU) Nº 910/2014.
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado de selo eletrónico.
Assinatura Eletrónica Qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Certificado de Autenticação de Sítio Web Qualificado	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo IV do Regulamento (EU) Nº 910/2014.
Relying Party	Qualquer pessoa singular ou entidade legal que confia num certificado válido.
Entidade de Registo (ER)	Entidade principalmente responsável pela identificação e autenticação de sujeitos de certificados. A ER pode apoiar no processo de solicitação de certificado, processo de revogação, ou em ambos.
EC Raiz	Entidade Certificadora de raiz, cujo certificado de raiz é distribuído por fornecedores de aplicações de software, e que emite certificados de Entidade Certificadora intermédia.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Dados de Criação de Assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dispositivo de Criação de Assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo Seguro de Criação de Assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Assunto	Pessoa singular, dispositivo, sistema, unidade ou entidade legal identificada num certificado como Assunto. O Assunto pode ser o subscritor/titular ou um dispositivo sob o controlo e operação de um subscritor.
EC Intermédia / Subordinada	Entidade Certificadora cujo certificado é assinado pela Entidade Certificadora Raiz, ou outra Entidade Certificadora Subordinada. Uma EC Subordinada normalmente emite certificados para utilizadores ou certificados para outras EC`s Subordinadas.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Subscritor	Pessoa singular ou entidade legal para a qual um certificado é emitido e que está legalmente vinculada por um contrato ou termos e condições.
Entidade Supervisora	Entidade responsável pelas tarefas de supervisão no respetivo Estado Membro, nomeadamente: - Supervisionar os prestadores qualificados de serviços de confiança estabelecidos no território do Estado-Membro que procede à designação por forma a garantir, por meio de atividades de supervisão a priori e a posteriori, que os prestadores e os serviços de confiança qualificados por eles prestados cumprem os requisitos estabelecidos no Regulamento 910/2014; - Se necessário, tomar medidas face aos prestadores de serviços de confiança não qualificados estabelecidos no território do Estado-Membro que procede à designação, por meio de atividades de supervisão a posteriori, se lhe for alegado que os ditos prestadores ou os serviços de confiança por eles prestados não cumprem os requisitos estabelecidos no Regulamento 910/2014.
Validação de Selo Temporal	Declaração da entidade certificadora, que certifica a data e hora de criação, envio, ou receção de um documento eletrónico.
Prestador de Serviços de Confiança (PSC ou TSP)	Pessoa singular ou entidade legal que fornece um ou mais serviços de confiança, como prestador de serviços de confiança qualificados ou não qualificados.

1.6.2 Acrónimos

Acrónimos	Definição
ANSI	American National Standards Institute
BR	Baseline Requirements
CA	Certification Authority

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

CAA	Certification Authority Authorization
CAB	Conformity Assessment Body
CLMS	Certificates Lifecycle Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DL	Decree-law
DN	Distinguished Name
EAL	Evaluation Assurance Level
MAC	Message Authentication Codes
NCA	National Competent Authority
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object identifier
OVCP	Organizational Validation Certificate Policy
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QEVCP-w	Certificate policy for EU qualified website authentication certificates based on EVCP

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

QSCD	Qualified electronic Signature/Seal Creation Device
SSCD	Secure Signature-Creation Device
TSA	Time-Stamping Authority (TSA)
TSP	Trust Service Provider

1.6.3 Referências Bibliográficas

Regulation EU No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on for electronic transactions in the internal market and repealing Directive 1999/93/EC

CA/Browser Forum, v1.8.6 – Baseline Requirements;

CA/Browser Forum, v1.8.0 – Guidelines for The Issuance and Management of Extended Validation Certificates;

Decreto-Lei nº 12/2021 – Assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;

Despacho 154/2017 da Entidade Supervisora nacional, de 5 de dezembro – Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência;

Despacho 155/2017 da Entidade Supervisora nacional, de 5 de dezembro – Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário;

CWA 14167 - Cryptographic Module for CSP Signing Operations - Protection Profile;

CWA 14169:2004 - Secure signature-creation devices "EAL 4+";

ETSI EN 319 401, v2.3.1 (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

ETSI EN 319 411-1, v1.3.1 (2021-05) - Electronic Signatures and Infrastructures (ESI); Policy and security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

ETSI EN 319 411-2, V2.4.1 (2021-11) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;

ETSI TS 119 412-1, v1.4.1 (2020-07) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

ETSI EN 319 412-1, v1.4.4 (2021-05) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

ETSI EN 319 412-2, v2.2.1 (2020-07) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

ETSI EN 319 412-3, V1.2.1 (2020-07) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

ETSI EN 319 412-4, V1.2.1 (2021-11) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
ETSI EN 319 412-5, v2.3.1 (2020-04) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
ETSI EN 319 421, v1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
ETSI EN 319 422, v1.1.1 (2016-03) – Electronic Signatures and Infrastructure (ESI); Time-stamping protocol and time-stamp token profiles;
ETSI TS 119 495, v1.6.1 (2022-11) – Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;
CEN/TS 419 241 v2014 – Security Requirements for Trustworthy Systems Supporting Server Signing;
FIPS 140-1. 1994, Security Requirements for Cryptographic Modules.
ISO/IEC 3166. 1997, Codes for the representation of names and countries and their subdivisions.
ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.
NIST FIPS PUB 180-1. 1995, The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce.
RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.
RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.
RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.
RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.
RFC 6960. 2013, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.
RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
RFC 4510. 2006, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.
RFC 4210. 2005, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).
RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
RFC 6844. 2013, DNS Certification Authority Authorization (CAA) Resource Record.
RFC 6962. 2013, Certificate Transparency.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

As EC`s abrangidas por esta política devem assegurar que os dados de revogação de certificados emitidos estão disponíveis publicamente através de um repositório 24 horas por dia, 7 dias por semana, com uma disponibilidade mínima de 99%.

As EC`s abrangidas por esta política devem disponibilizar publicamente a PC e DPC, que devem ser atualizadas anualmente.

2.2 Publicação de Informação de Certificado

A informação pública da PKI Multicert está disponível na internet, no repositório disponível em https://pki.multicert.com.

2.3 Periodicidade de Publicação

As atualizações a esta PC e DPC correspondente devem ser publicadas até 7 dias após a sua aprovação.

Os certificados das EC`s geridas pela Multicert devem ser publicados logo que possível após a sua emissão.

As CRL`s emitidas pela EC Raiz da Multicert devem ser publicadas logo que possível após a sua emissão.

As CRL`s emitidas por EC`s Subordinadas da Multicert devem ser publicadas imediatamente após a sua emissão.

2.4 Controlo de Acesso aos Repositórios

A informação publicada pela Multicert deve estar disponível na internet, sendo sujeita a mecanismos de controlo de acesso (acesso apenas de leitura).

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

3 Identificação e Autenticação

3.1 Atribuição de Nomes

3.1.1 Tipos de Nomes

Os certificados da Multicert devem ser emitidos de acordo com o standard ITU X.500 e os seus Nomes Distintos (*Distinguished Name* – DN) devem ser construídos de acordo com a ETSI EN 319 412-1, ETSI EN 319 412-2 no caso de certificados para pessoa singular, ETSI EN 319 412-3 no caso de certificados para pessoa coletiva, e ETSI EN 319 412-4 no caso dos certificados para autenticação de *website*.

3.1.2 Necessidade de Nomes Significativos

Os tipos de certificados descritos neste documento devem ser emitidos utilizando Nomes Únicos de forma a clarificar um nome único e identificável. Podem ser usados alguns atributos para tornar os nomes significativos. Um exemplo desses atributos é o *serial number* e o *organization identifier*.

3.1.3 Anonimato ou Pseudónimo de Subscritores/Titulares

Os tipos de certificados descritos neste documento podem ser emitidos com pseudónimos em casos específicos, desde que esta informação seja fornecida no certificado e que toda a validação sobre a autenticidade do Subscritor seja corretamente realizada.

3.1.4 Regras para Interpretação de Formato de Nomes

As regras utilizadas pela Multicert para interpretar o formato dos nomes devem seguir o estabelecido no RFC 5280[1], assegurando que todos os atributos DirectoryString dos campos "*issuer*" e "*subject*" do certificado são codificados no formato UTF8String, com exceção dos atributos "*country*" e "*serialnumber*" que são codificados no formato PrintableString.

3.1.5 Unicidade de Nomes

Todos os certificados emitidos segundo esta política têm um número de série que fornece a sua unicidade. No caso dos certificados SSL/QWAC, a unicidade do nome de domínio é controlada pelo *Internet Corporation for Assigned Names and Numbers* (ICANN).

[1] cf. RFC 5280. 2008, InternetX.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

3.1.6 Reconhecimento, Autenticação, e Função de Marcas Registadas

Os Subscritores não podem solicitar certificados com conteúdos que infrinjam os direitos de propriedade intelectual de uma terceira parte. A emissão de um certificado com uma marca registada é sempre sujeita a uma verificação meticulosa.

3.2 Validação de Identidade Inicial

Os certificados emitidos segundo esta política são sempre sujeitos a uma verificação meticulosa do indivíduo e/ou organização para a qual o certificado vai ser emitido.

3.2.1 Método de Prova de Posse da Chave Privada

No caso de o Subscritor gerar a chave privada, a EC que vai emitir o certificado deve confirmar a posse da chave privada no pedido de certificado (*Certificate Signing Request* – CSR). Se se tratar de um certificado qualificado, a chave deve ser gerada e armazenada num QSCD (*Qualified Secure Cryptographic Provider*).

3.2.2 Autenticação de Identidade da Organização

Para todos os certificados que incluem a identidade de uma organização, devem ser validados os dados da pessoa legal utilizando uma das formas descritas na DPC.

No caso dos certificados SSL, deve ser verificada a autoridade do Subscritor para solicitar o certificado em nome da organização de acordo com a secção 3.2.5 das *Baseline Requirements*.

Quando é incluído um nome de domínio no certificado, a Multicert deve autenticar o direito da Organização para utilizar o nome de domínio como um *fully qualified domain name*. Nestes casos, é necessária a confirmação do controlo do domínio, utilizando um dos métodos descritos na secção 3.2.2.2 da DPC.

3.2.2.1 Método de Prova de Controlo de Endereço de Email

Quando o endereço de email é incluído nos atributos do *Distinguished Name* ou *Subject Alternative Name* do certificado, o Subscritor deve fazer prova de controlo do endereço de email a ser incluído no certificado.

3.2.2.2 Método de Validação de Controlo de Nome de Domínio / Endereço IP

A EC deve confirmar que, à data da emissão do certificado, o Subscritor do certificado é o responsável pelo nome de domínio ou tem controlo sobre o *Full Qualified Domain Name*, através dos procedimentos descritos na secção 3.2.2.2 da DPC.

3.2.3 Autenticação de Identidade do Indivíduo

A EC emissora de certificados deve confirmar a autenticidade da identidade do indivíduo. Para tal, utiliza uma das formas de validação de identidade descritas na secção 3.2.3 da DPC.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Sempre que um endereço de email é incluído nos atributos do *Distinguished Name* ou *Subject Alternative Name* do certificado digital, o subscritor deve provar o controlo do email conforme descrito na secção 3.2.2.1.

3.2.4 Informação do Subscritor/Titular Não Verificada

Toda a informação fornecida pelo Subscritor deve ser verificada antes da emissão do certificado.

3.2.5 Validação de Autoridade

A autoridade do indivíduo que solicita o certificado em nome do Subscritor, quando o Subscritor é uma Organização, deve ser verificada de acordo com os métodos descritos na secção 3.2.5 da DPC.

3.2.6 Critérios para Interoperabilidade

Os certificados emitidos segundo esta política são emitidos debaixo de uma só hierarquia de confiança da Multicert.

No caso dos certificados SSL, a EC Multicert responsável pela emissão de certificados SSL foi alvo de certificação cruzada de forma a garantir o reconhecimento da Mozilla.

3.3 Identificação e Autenticação para Pedidos de *Re-Key*

3.3.1 Identificação e Autenticação para Pedidos de Rotina de *Re-Key*

A Multicert requer ao Subscritor que use os mesmos detalhes de autenticação usados no pedido original de pedido de certificado.

3.3.2 Identificação e Autenticação para *Re-Key* após Revogação

Todos os pedidos após revogação são tratados como novas emissões de certificados, sujeitos ao mesmo procedimento de validação inicial.

3.4 Identificação e Autenticação para Pedido de Revogação

Os pedidos de revogação devem ser feitos de forma autenticada, ou de outra forma garantindo a validação da autenticidade do pedido.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de Certificado

4.1.1 Quem Pode Submeter um Pedido de Certificado

Tanto o Subscritor/Titular como um indivíduo autorizado pelo Subscritor podem submeter um pedido de certificado. Os Subscritores são responsáveis pelos dados que o Subscritor ou um indivíduo autorizado pelo Subscritor submeta à Multicert.
O pedido de certificado deve ser acompanhado por um Formulário de Pedido de Certificado preenchido.

4.1.2 Processo de Registo e Responsabilidades

A Entidade de Registo é responsável por verificar o processo de registo de acordo com o definido na PC e DPC, antes de submeter o pedido para emissão de certificado pela EC.

1. O Subscritor ou um indivíduo autorizado pelo Subscritor é responsável por submeter a informação e documentação necessária, de forma completa e precisa, para permitir à ER proceder às validações necessárias antes da emissão do certificado.

4.2 Processamento do Pedido de Certificado

4.2.1 Desempenhando Funções de Identificação e Autenticação

As EC`s e ER`s devem identificar e verificar de forma auditável todos os pedidos de certificado de acordo com as secções 3.2 e 3.3 da DPC.

4.2.2 Aprovação ou Rejeição de Pedidos de Certificado

Todos os pedidos que sejam identificados e verificados com sucesso, são aprovados para emissão pela EC emissora.

Caso não seja possível verificar o pedido a EC emissora deve rejeitar a emissão do certificado.

4.2.3 Prazo de Processamento de Pedidos de Certificado

Uma vez verificado com sucesso o pedido a EC emite o certificado de acordo com o SLA acordado, cuja informação está disponível na loja online.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.3 Emissão de Certificado

4.3.1 Ações da EC durante a Emissão do Certificado

As EC`s/ER`s verificam os dados dos pedidos antes de procederem à emissão do certificado, de acordo com o estipulado na secção 3.2 da DPC.

Todos os sistemas pertencentes ao processo de emissão de certificado devem ser protegidos contra modificação, através de políticas de controlo de acesso, proteção das bases de dados, autenticação entre sistemas, etc.

Quando a emissão do certificado envolve a EC Raiz, são necessários elementos autorizados pertencentes aos grupos de trabalho a fim de emitir manualmente o certificado na EC Raiz.

4.3.2 Notificação ao Subscritor/Titular pela EC Emissora do Certificado

As EC`s emissoras devem notificar o Subscritor por email quando o seu certificado é emitido.

4.4 Aceitação do Certificado

4.4.1 Conduta que Constitui a Aceitação do Certificado

Os certificados são considerados aceites 7 dias após a sua emissão, ou antes se o certificado for usado quando exista evidência de que o Subscritor usou o certificado.

4.4.2 Publicação do Certificado pela EC

Os certificados de EC`s emitidas pela Multicert são publicados no seu repositório.

Os certificados de Subscritores são publicados através da entrega do certificado ao Subscritor.

4.4.3 Notificação da Emissão do Certificado pela EC a Outras Entidades

Podem ser informados da emissão de certificado as ER`s Multicert ou parceiros/revendedores caso estejam envolvidos na solicitação inicial do certificado.

No caso dos certificados PSD2, pode ser notificada a NCA do país do Subscritor caso esta tenha indicado essa intenção previamente à Multicert.

4.5 Utilização do Certificado e Par de Chaves

4.5.1 Utilização do Certificado e Par de Chaves pelo Subscritor/Titular

O Subscritor deve usar as suas chaves privadas de acordo com os termos e condições aceites e de acordo com a PC e DPC.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

As chaves privadas são pessoais de tal forma que o Subscritor não pode torná-las disponíveis para terceiras partes.

As chaves privadas apenas devem ser usadas para a finalidade exclusiva a que se destinam.

4.5.2 Utilização do Certificado e Chave Pública pela *Relying Party*

As *Relying Parties* devem verificar sempre a validade do certificado e o seu estado através dos métodos disponibilizados pela EC, tais como as CRL`s e OCSP.

4.6 Renovação de Certificado

A renovação de certificado refere-se à emissão de um novo certificado para o Subscritor, sem alteração da chave pública nem da informação contida no certificado.

4.6.1 Circunstâncias para a Renovação do Certificado

Um certificado pode ser substituído pela Multicert por sua iniciativa, ou pode ser renovado por iniciativa do Subscritor nas situações descritas na secção 4.6.1 da DPC.

4.6.2 Quem Pode Solicitar a Renovação

A EC pode iniciar a renovação do certificado por sua iniciativa, após notificar o Subscritor do certificado.
O Subscritor pode solicitar a renovação do certificado nas condições descritas na secção 4.6.1 da DPC.

4.6.3 Processamento de Pedidos de Renovação de Certificado

Quando ocorre a renovação do certificado, o par de chaves, a data *Not After*, e os dados do *Distinguished Name* e *Subject Alternative Name* do certificado mantém-se os mesmos que a primeira emissão. Por esse motivo, a Multicert reutiliza por sua iniciativa a informação anteriormente verificada dentro dos limites de reutilização de informação descritos na secção 4.6.1 da DPC.
Quando ocorre a substituição do certificado, os dados do *Distinguished Name* e/ou *Subject Alternative Name* podem mudar. Neste caso, são realizadas validações adicionais se necessário de acordo com o descrito na DPC.

4.6.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A EC deve notificar o Subscritor em tempo razoável após a emissão do certificado e pode usar qualquer mecanismo confiável para entregar o certificado ao Subscritor.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.6.5 Conduta que Constitui a Aceitação do Certificado Renovado

Os certificados renovados são considerados aceites 7 dias após a sua entrega ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.6.6 Publicação do Certificado Renovado pela EC

Ver secção 4.4.2.

4.6.7 Notificação do Certificado Emitido pela EC a Outras Entidades

Ver secção 4.4.3.

4.7 *Re-Key* de Certificado

Fazer *Re-Key* de um certificado consiste em criar um novo certificado com uma nova chave pública.

4.7.1 Circunstâncias para *Re-Key* de Certificado

Os pedidos de *re-key* devem ser identificados e autenticados de acordo com o definido na secção 3.3.

4.7.2 Quem Pode Solicitar a Certificação de uma Nova Chave Pública

A Multicert pode aceitar um pedido de *re-key* de um certificado desde que seja proveniente do Subscritor do certificado ou de um Representante da Entidade/Organização, quando aplicável, ou pode proceder ao re-key de um certificado por sua iniciativa quando verifique que o certificado emitido não cumpre com os requisitos definidos no respetivo perfil de certificado ou DPC.

4.7.3 Processamento de Pedidos de *Re-Key* de Certificado

A Multicert pode solicitar informação adicional antes de processar um *re-key* e pode validar novamente o Subscritor para verificar novamente quaisquer dados previamente validados, se necessário.
O novo certificado emitido é enviado através de um meio de comunicação confiável previamente verificado.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.7.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A EC deve notificar o Subscritor num prazo razoável após a emissão do certificado.

4.7.5 Conduta que Constitui a Aceitação do Certificado para o qual foi feito *Re-Key*

Os certificados emitidos são considerados aceites 7 dias após ser feito *re-key* do certificado, ou antes caso exista evidência de utilização do certificado pelo Subscritor.

4.7.6 Publicação do Certificado pela EC para o qual foi feito *Re-Key*

A EC publica os certificados para os quais foi feito *re-key*, entregando-os ao Subscritor.

4.7.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Sem Estipulação.

4.8 Modificação de Certificado

A modificação de certificado refere-se à emissão de um novo certificado devido a alterações na informação do certificado que não a chave pública do Subscritor.

4.8.1 Circunstâncias para a Modificação de Certificado

Um certificado pode ser modificado por iniciativa da Multicert quando se verifica que este não cumpre com os requisitos definidos no respetivo perfil de certificado ou DPC.
Os certificados podem ser modificados se:

- O certificado não está expirado nem revogado.

4.8.2 Quem Pode Solicitar a Modificação de Certificado

A Multicert pode iniciar a modificação de um certificado por sua iniciativa, após notificar o Subscritor do certificado.

4.8.3 Processamento de Pedidos de Modificação de Certificado

Quando a modificação do certificado incide sobre os dados constantes no *Distinguished Name* e/ou *Subject Alternative Name*, a Multicert realiza validações adicionais dos dados a serem alterados. Quando são efetuadas outras alterações que não os dados do *Distinguished Name*

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

e/ou *Subject Alternative Name*, a Multicert reutiliza a informação do pedido de certificado inicial. A validade do certificado modificado nunca é superior à validade do certificado inicial.

4.8.4 Notificação de Nova Emissão de Certificado ao Subscritor/Titular

A Multicert notifica o Subscritor em tempo razoável após a emissão do certificado.

4.8.5 Conduta que Constitui Aceitação de Certificado Modificado

Os certificados modificados são considerados aceites 7 dias após a sua entrega ou notificação da emissão do certificado ao Subscritor, ou quando exista evidência de que o Subscritor utilizou o certificado.

4.8.6 Publicação do Certificado Modificado pela EC

Ver secção 4.4.2.

4.8.7 Notificação de Emissão de Certificado pela EC a Outras Entidades

Ver secção 4.4.3.

4.9 Revogação e Suspensão de Certificado

4.9.1 Motivos para Revogação

A revogação ou suspensão de certificados são ações através das quais o certificado perde a sua validade antes do término do período de validade, perdendo a sua operacionalidade.

Certificados no estado suspenso podem ser revertidos para o estado ativo. Certificados no estado revogado não podem ser revertidos para o estado ativo.

Se uma das seguintes razões ocorrer, o certificado deve ser revogado dentro de 24 horas:

- O Subscritor solicita à EC a revogação do certificado, através da submissão de um formulário de pedido de revogação;
- O Subscritor notifica a EC de que o pedido original de certificado não foi autorizado e não concede autorização com efeitos retroativos;
- A chave privada e/ou a password de acesso à chave privada (i.e. PIN) foi comprometido ou existe suspeita de comprometimento;
- A chave privada foi perdida;
- A EC tem conhecimento de um método demonstrado ou comprovado que pode facilmente computar a chave privada do Subscritor com base na chave pública do certificado;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

- A EC obtém evidência de que a validação da autorização ou controlo do domínio de qualquer nome de domínio qualificado ou endereço IP do certificado não deve ser considerada.

Se uma das seguintes razões ocorrer, o certificado deve ser revogado dentro de 5 dias:

- O certificado foi usado para finalidades não autorizadas;
- A EC é informada de uma alteração significativa na informação contida no certificado;
- A EC determina ou tem conhecimento de que qualquer informação do certificado é imprecisa;
- A EC tem conhecimento de que o Subscritor violou uma ou mais obrigações estipuladas nos termos e condições de emissão do certificado digital;
- A EC tem conhecimento de que o certificado não foi emitido de acordo com os requisitos da EC previstos na DPC, PC ou requisitos normativos aplicáveis;
- O algoritmo e tamanho de chave do certificado, ou a geração e verificação da qualidade dos parâmetros da chave pública já não estão em conformidade com a ETSI TS 119 312;
- A EC tem conhecimento de quaisquer circunstâncias que indiquem que a utilização do nome de domínio qualificado ou endereço IP do certificado já não são legalmente permitidos (ex: foi revogado pelo tribunal o direito de uso do nome de domínio ao *Domain Name Registrant*, foi rescindido um licenciamento ou contrato de serviços relevante entre o *Domain Name Registrant* e o Subscritor, ou o *Domain Name Registrant* falhou a renovação do nome de domínio);
- A EC tem conhecimento de um método demonstrado ou comprovado que expõe ao comprometimento da chave privada do Subscritor, foram desenvolvidos métodos que podem calcular facilmente a chave privada com base na chave pública (como uma chave fraca Debian, ou se houver evidência de que o método específico usado para gerar a chave privada tinha falhas;
- Quando aplicável, se o token/smartcard criptográfico onde a chave privada está armazenada tenha sido perdido, destruído ou deteriorado.

Se uma das seguintes razões ocorrer, o certificado pode ser revogado pela EC:

- A EC é notificada devido a uma resolução legal ou administrativa;
- A EC tem conhecimento de que o certificado foi usado para atividades ilícitas;
- A EC cessa funções e não encontra outra EC que forneça suporte à revogação dos certificados.

Se uma das seguintes razões ocorrer, o certificado PSD2 pode ser revogado a pedido da NCA:

- A NCA retira um ou mais papéis ao PSP, que estavam incluídos no certificado;
- A NCA retira a autorização PSD2 ao PSP que solicitou o certificado.

Se uma das seguintes razões ocorrer, a EC Subordinada é revogada dentro de 7 dias:

- A EC Subordinada solicita a revogação por escrito;
- A EC Subordinada notifica a EC Emissora de que o pedido de certificado original não foi autorizado e não concede autorização com efeitos retroativos;
- A EC Emissora obtém evidência de que a chave privada da EC Subordinada que corresponde à chave pública no certificado sofreu um comprometimento ou já não está em conformidade com a ETSI TS 119 312;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

- A EC Emissora obtém evidência de que o certificado foi usado para finalidades não autorizadas;
- A EC Emissora tem conhecimento de que o certificado não foi emitido de acordo com ou a EC Subordinada não cumpriu com os requisitos Baseline Requirements ou PC ou DPC aplicáveis, no caso dos certificados QWAC;
- A EC Emissora determina que qualquer informação constante no certificado é imprecisa ou enganadora;
- A EC Emissora ou a EC Subordinada cessa funções por qualquer razão e não tem acordos com outra EC para o fornecimento de suporte à revogação do certificado;
- É requerida revogação pela DPC e/ou PC da EC Emissora.

4.9.2 Quem Pode Solicitar Revogação

A EC ou ER devem aceitar pedidos de revogação provenientes de partes autenticadas e autorizadas, tais como o Subscritor ou a Entidade/Organização associada, quando aplicável. A EC ou ER podem estabelecer procedimentos que permitam outras entidades solicitar a revogação do certificado, tais como a NCA no caso dos certificados PSD2.

4.9.3 Procedimento para o Pedido de Revogação

A EC deve fornecer um processo para os Subscritores solicitarem a revogação dos seus próprios certificados. O processo deve ser descrito na DPC da EC.

A EC deve revogar sempre o certificado se o pedido for autenticado como originário pelo Subscritor ou Entidade/Organização associada, quando aplicável.

4.9.4 Período de Carência do Pedido de Revogação

O período de carência do pedido de revogação é o tempo disponível para o Subscritor tomar as ações necessárias para pedir a revogação de um certificado sobre o qual exista suspeita de comprometimento da chave, utilização de uma chave fraca ou descoberta de informação imprecisa contida no certificado.

Nesta situação, o Subscritor deve pedir a revogação dentro de 24 horas após a sua deteção.

4.9.5 Tempo de Processamento do Pedido de Revogação pela EC

A EC deve revogar o certificado dentro de 24 horas quando o pedido é feito através de formulário de pedido revogação escrito. Quando o pedido de revogação é feito de forma autenticada, a revogação deve ser processada imediatamente.

4.9.6 Requisito de Verificação da Revogação pelas *Relying Parties*

As *Relying Parties* devem confirmar a validade do certificado através dos serviços que a EC tenha disponibilizado, tais como o OCSP e CRL, de acordo com o definido na secção 4.9.6 da DPC.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.9.7 Frequência de Emissão de CRL

As EC`s a funcionarem de acordo com esta política devem emitir CRL`s com a seguinte frequência:

- EC`s Intermédias/Subordinadas – diariamente é emitida CRL e a cada 12 horas é emitida Delta CRL;
- EC Raiz – a cada 12 meses ou dentro de 24 horas se for revogado o certificado de uma EC Subordinada.

4.9.8 Latência Máxima para CRLs

AS CRL`s de certificados emitidos para utilizadores finais devem ser publicadas automaticamente no repositório online, dentro de um prazo comercialmente razoável após a sua geração, tipicamente dentro de minutos após a sua geração.
Quando são emitidas CRL`s da EC Raiz devido à revogação de uma EC Subordinada, a CRL deve ser publicada dentro de 24 horas após a sua emissão. As CRL`s regularmente agendadas são publicadas antes do campo *nextUpdate* da CRL anteriormente emitida para o mesmo âmbito.

4.9.9 Disponibilidade de Verificação de Estado/Revogação *On-Line*

Todas as EC`s abrangidas por esta política devem fornecer serviço OCSP.

As respostas OCSP devem ser conformes com o RFC 6960 ou RFC 5019. As respostas OCSP devem ser sempre assinadas pela EC que emitiu o certificado cujo estado de revogação está a ser verificado.

4.9.10 Requisitos de Verificação de Revogação *On-Line*

A *Relying Party* deve confirmar a validade do certificado de acordo com a seção 4.9.6 antes de confiar no certificado.

Os OCSP *responders* que recebam um pedido de estado de um certificado que ainda não foi emitido, não devem responder com o estado "*good*" para tal certificado.

4.9.11 Outras Formas Disponíveis de Anunciar Revogação

Sem Estipulação.

4.9.12 Requisitos Especiais Relacionados com o Comprometimento de Chave

A EC ou ER devem usar métodos comercialmente razoáveis para informar potenciais *Relying Parties* se descobrirem ou suspeitarem que a chave privada foi comprometida. A EC deve ter a capacidade de fazer a transição de qualquer motivo de revogação para o código de "*key compromise*".

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

A comunicação de uma chave privada comprometida deve ser efetuada de acordo com o estipulado na secção 4.9.12 da DPC.

4.9.13 Motivos para a Suspensão

É permitida a suspensão de certificado, exceto no caso dos certificados QWAC.

4.9.14 Quem Pode Solicitar Suspensão

A EC e a ER devem aceitar pedidos de suspensão autenticados. A autorização para a suspensão deve ser aceite se o pedido de suspensão for efetuado pelo Subscritor ou Entidade/Organização associada, quando aplicável. A EC também pode suspender o certificado por sua iniciativa.

4.9.15 Procedimento para o Pedido de Suspensão

Considerando a natureza dos pedidos de suspensão e a necessidade de eficiência, a EC e a ER providenciam mecanismos automáticos para a solicitação e autenticação de pedidos de suspensão.

4.9.16 Limites do Período de Suspensão

O limite do período de suspensão depende do meio utilizado para suspender o certificado. Os limites do período de suspensão encontram-se definidos na secção 4.9.16 da DPC.

4.10 Serviços de Estado de Certificado

4.10.1 Características Operacionais

A EC deve disponibilizar informação sobre o estado do certificado via CRL e OCSP. A EC deve listar os certificados revogados na CRL apropriada, e devem ser mantidos após a data de expiração.

4.10.2 Disponibilidade de Serviço

Os serviços de estado do certificado devem estar disponíveis 24 horas por dia, 7 dias por semana.

4.10.3 Funcionalidades Opcionais

Sem Estipulação.

4.11 Fim de Subscrição

A EC deve permitir aos Subscritores terminarem a sua subscrição dos serviços de certificado tendo o seu certificado revogado, permitindo que o certificado expire sem renovação, ou permitindo que o contrato do subscritor expire sem renovação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

4.12 Custódia e Recuperação de Chaves

4.12.1 Política e Práticas de Custódia e Recuperação de Chaves

A PKI Multicert não faz custódia de chaves de certificados para utilizador final.

A PKI Multicert pode fazer custódia de chaves para chaves privadas de EC`s, neste caso é planeada e realizada uma cerimónia pelos membros dos grupos de trabalho necessários de acordo com os artefactos necessários para esta operação.

4.12.2 Política e Práticas de Encapsulamento e Recuperação de Chave de Sessão

Sem Estipulação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5 Controlos de Segurança Física, Gestão e Operacionais

As EC`s devem implementar várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta PC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos Subscritores/Titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falha de segurança pode comprometer as operações da EC.

5.1 Controlos de Segurança Física

5.1.1 Localização Física e Tipo de Construção

As instalações das EC`s devem ser desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas de acesso não autorizado, dano ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

As operações devem ser realizadas numa sala em zona de alta segurança, inserida noutra zona também de alta segurança, e dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

As duas zonas de alta segurança são áreas que devem obedecer às seguintes características:

a) Paredes em alvenaria, betão ou tijolo;
b) Tecto e pavimento com construção similar à das paredes;
c) Inexistência de janelas;
d) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreiras igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta-fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança devem ser garantidas:

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, betão ou tijolo sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras antirroubo de alta segurança, nas portas de acesso ao ambiente de segurança;
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

- O acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso Físico

Os sistemas devem ser protegidos por, no mínimo, 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança), garantindo que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

As atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação, e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação. Os acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

O acesso ao cartão de identificação obrigada a um duplo controlo de autenticação de acesso individual. Ao pessoal não acompanhado, incluindo colaboradores ou visitantes não autenticados, não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é obrigatório o uso do respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer, no mínimo, dois fatores de autenticação, incluindo autenticação biométrica. O hardware criptográfico e tokens físicos seguros dispõem de proteção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita de alta segurança, assim como ao hardware criptográfico e aos tokens físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

5.1.3 Energia e Ar Condicionado

O ambiente seguro deve possuir equipamento redundante, que garanta condições de funcionamento 24 horas por dia, 7 dias por semana, de:

- Fornecimento de energia elétrica ininterrupta com a potência suficiente para manter autonomamente a disponibilidade de serviço durante períodos de falta de abastecimento da rede pública. O sistema garante a proteção dos equipamentos face a flutuações elétricas que os possam danificar (a alternativa à rede pública é garantida por unidades de alimentação ininterrupta e baterias, bem como geradores de eletricidade a diesel); e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. A desconformidade dos parâmetros de temperatura/humidade despoleta o envio de alarmes para as equipas de manutenção e para a Central de Segurança.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.1.4 Exposição à Água

As zonas de alta segurança têm instalados os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da EC.

5.1.5 Prevenção e Proteção contra Incêndio

O ambiente Seguro tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Estão instalados nos vários níveis físicos de segurança, sistemas de deteção e alarme de incêndio;
- Estão disponíveis equipamentos fixos e móveis de extinção de incêndios, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Existem procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Armazenamento de *Media*

Todos os suportes de informação sensível, contendo software e dados de produção, informação para auditoria, arquivo ou cópias de segurança são guardados em confres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício, com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além das restrições de acessos, também estão implementados mecanismos de proteção contra acidentes (e.g. causados por água ou fogo).

Quando, para efeitos de arquivo de cópias de segurança, é transportada informação sensível da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo menos 2 elementos do Grupo de trabalho que têm por obrigação garantir o transporte seguro da informação até ao local de destino. A informação (ou o token de transporte da informação) deverá estar sempre sob controlo visual dos membros do Grupo de Trabalho.

Em situações que impliquem a deslocação física de hardware de armazenamento de dados (i.e. discos rígidos) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento de hardware deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser eliminada usando todos os meios necessários para o efeito (formatação do disco rígido, *reset* do hardware criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de Resíduos

Os documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação “segura” de baixo nível ou destruição física), antes dos mesmos serem eliminados. Os equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

recomendações de destruição do respetivo fabricante, antes da sua eliminação. Os outros equipamentos de armazenamento (como discos rígidos ou *tapes*) devem ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 *Backup* em Instalações Externas

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físico e lógico, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a proteção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Controlos Procedimentais

A atividade de uma EC depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC, é vital garantir uma adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes;
- É necessário garantir que a EC apenas poderá ser sujeita a ataques do tipo *denial-of-service* mediante o conluio de um número significativo de intervenientes.

Por este motivo, nesta secção descrevem-se os papéis de confiança e responsabilidades associadas a cada um desses papéis.

5.2.1 Grupos de Trabalho

Definem-se como pessoas autenticadas todos os colaboradores, fornecedores e consultores que tenham acesso ou que controlem operações criptográficas ou de autenticação.

A Multicert estabeleceu que os papéis de confiança fossem agrupados em 8 (oito) categorias diferentes (que correspondem a 6 Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticadas, pertencentes a diferentes Grupos de Trabalho.
Não estão autorizadas entradas no “Ambiente de Produção” sem a presença mínima de dois elementos, pertencentes a Grupos de Trabalho distintos (com exceção do Grupo de trabalho de Custódia que não tem permissão para aceder a este ambiente).
Como medida adicional de segurança, a Multicert considera relevante, mas não mandatória, a presença em todas as intervenções de um elemento de Auditoria.

5.2.1.1 Grupo de Trabalho de Operação

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.2.1.2 Grupo de Trabalho de Autenticação

É responsável por assegurar a gestão, salvaguarda e disponibilidade de passwords e *tokens* de autorização (não pessoais), e a definição, atualização, e proposta de políticas das EC`s ao Grupo de Trabalho de Gestão.

5.2.1.3 Grupo de Trabalho de Auditoria

É responsável por efetuar a auditoria interna de todas as ações relevantes e necessárias para assegurar a operacionalidade das EC`s.

5.2.1.4 Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (tokens de autenticação, entre outros), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

5.2.1.5 Grupo de Trabalho de Operação de Registo

É responsável por validar a documentação relacionada com o pedido de certificado, assegurar a emissão, renovação, suspensão e revogação de certificados.

5.2.1.6 Grupo de Trabalho de Administração de Sistemas

É responsável pela instalação, configuração e manutenção dos sistemas da PKI (hardware e software). É também responsável pela consolidação e análise da monitorização dos pontos de controlo de segurança de todos os recursos utilizados na PKI da MULTICERT, que podem dar origem a eventos, alarmes e incidentes.

5.2.1.7 Grupo de Trabalho de Gestão

É o órgão de decisão da PKI Multicert.

A missão do Grupo de trabalho de Gestão assenta principalmente na tomada de decisões importantes e críticas ao bom funcionamento da EC Multicert, realçando a revisão e aprovação de todos os documentos e políticas das EC`s propostas pelo Grupo de Trabalho de Autenticação. O Grupo de Trabalho de Gestão tem ainda como missão a nomeação e/ou destituição dos membros dos restantes grupos e a guarda de alguns artefactos sensíveis (tokens de autenticação, entre outros).

5.2.1.8 Grupo de Trabalho de Manutenção

É responsável por assegurar o acompanhamento e supervisão de ações de manutenção e limpeza das salas do CPD.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.2.2 Número de Pessoas Exigidas por Tarefa

Existem procedimentos e controlo rigorosos que obrigam à divisão de responsabilidades baseadas nas especificidades de cada Grupo de Trabalho, e de modo a garantir que tarefas sensíveis apenas podem ser executadas por um conjunto múltiplo de pessoas autenticadas.

Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao hardware criptográfico das EC`s segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do hardware. Após a ativação de um módulo com chaves operacionais, são utilizados controlos adicionais de acesso de modo a garantir que os acessos físicos e lógicos ao hardware só são possíveis com 2 ou mais indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

5.2.3 Identificação e Autenticação por Função

O pessoal afeto à EC deve-se autenticar no sistema de gestão de certificados antes de terem acesso aos sistemas necessários para desempenhar as suas tarefas.

5.2.4 Funções que Requerem Separação de Responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por ✖) entre a pertença ao grupo identificado nas colunas e a pertença ao grupo identificado nas linhas, no contexto da EC:

Se pertence ao Grupo ...	**Pode pertencer ao Grupo?**	**Administração de Sistemas**	**Operação**	**Autenticação**	**Operação de Registo**	**Auditoria**	**Custódia**	**Gestão**	**Manutenção**
Administração de Sistemas				✖	✖	✖	✖	✖	
Operação				✖		✖	✖	✖	
Autenticação		✖	✖		✖	✖	✖	✖	✖
Operação de Registo		✖	✖	✖		✖	✖	✖	✖
Auditoria		✖	✖	✖	✖		✖	✖	✖
Custódia		✖	✖	✖	✖	✖		✖	✖
Gestão		✖	✖	✖	✖	✖	✖		✖
Manutenção				✖	✖	✖	✖	✖	

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.3 Controlos de Segurança Pessoal

A admissão de pessoal com funções de confiança nos Grupos de Trabalho apenas é possível se forem cumpridas as seguintes condições:

- Ser formalmente nomeado para a função;
- Ter recebido treino adequado para a função;
- Fazer prova da sua identidade, usando documentação emitida por fontes fiáveis;
- Fazer prova de não possuir antecedentes criminais;
- Fazer prova de que possui as qualificações e experiência exigidas pela entidade ou grupo que efetuou a sua a sua nomeação formal;
- Comprometer-se (formalmente) a não revelar (salvo com autorização expressa dos representantes legais da entidade que detém a EC) qualquer informação sobre a EC, o seu funcionamento, sobre os ambientes e recursos humanos ao seu serviço e sobre os titulares dos certificados digitais por esta emitidos;
- Comprometer-se (formalmente) a desempenhar as funções para as quais foi nomeado e a não assumir responsabilidades que possam colocar problemas éticos ou deontológicos à sua execução. Nesse sentido, é necessário que declare não só conhecer os termos e condições para o desempenho das respetivas funções, como também a sua capacidade e disponibilidade para o fazer.

5.3.1 Requisitos relativos a Qualificações, Experiência, e Autorização

A admissão de novos membros nos Grupos de Trabalho é apenas possível se apresentarem provas de conhecimento, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho.

5.3.2 Procedimentos de Verificação de Antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identidade, usando documentação emitida por fontes fiáveis; e
- Investigação de registos criminais.

5.3.3 Requisitos de Formação

É ministrado aos membros dos Grupos de Trabalho formação e treino adequado de modo a realizarem as suas tarefas, satisfatória e competentemente.

Os elementos dos Grupos de Trabalho estão sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

a) Certificação digital e Infraestruturas de Chave Pública;
b) Conceitos gerais sobre segurança da informação;
c) Formação específica para o seu papel dentro do Grupo de Trabalho;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

d) Funcionamento do software e/ou hardware usado pela EC;
e) Política de Certificado e Declaração de Práticas de Certificação;
f) Recuperação de desastres;
g) Procedimentos para a continuidade da atividade; e
h) Aspetos legais básicos relativos à prestação de serviços de certificação.

5.3.4 Frequência e Requisitos para Atualização de Formação

São realizadas ações de formação e treino, no mínimo, a cada 12 meses.

Sempre que necessário será ministrado treino e formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de profissionalismo para a execução competente e satisfatória das suas responsabilidades. Em particular:

- Sempre que existem alterações tecnológicas, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto à EC;
- Sempre que sejam introduzidas alterações na Política de Certificado ou Declaração de Práticas de Certificação são realizadas sessões de atualização de formação aos elementos da EC.

5.3.5 Frequência e Sequência da Rotação de Funções

Sem Estipulação.

5.3.6 Sanções para Ações Não Autorizadas

Consideram-se ações não autorizadas todas as que desrespeitem a Declaração de Práticas de Certificação e a Política de Certificado, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência.

São aplicadas sanções de acordo com as regras de trabalho, legislação nacional e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

5.3.7 Requisitos para Prestadores de Serviços Independentes

Consultores ou prestadores de serviços independentes têm permissão de acesso à zona de alta segurança desde que estejam sempre devidamente autorizados, acompanhados e diretamente supervisionados por elementos pertencentes aos Grupos de trabalho e após tomada de conhecimento e aceitação da Declaração de Confidencialidade.

5.3.8 Documentação Fornecida ao Pessoal

É disponibilizado aos membros dos Grupo de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas, de modo competente e satisfatório.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.4 Procedimentos de Registo de Auditoria

5.4.1 Tipos de Eventos Registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

- Pedido, emissão, renovação, reemissão e revogação de certificados;
- Publicação de CRL;
- Eventos relacionados com segurança, incluindo:
  - Tentativas de acesso (com e sem sucesso) a recursos sensíveis das EC`s;
  - Operações realizadas por membros dos Grupos de Trabalho;
  - Dispositivos físicos de segurança de entrada / saída dos vários níveis de segurança.

As entradas nos registos incluem a seguinte informação:

- Número de série do evento;
- Data e hora do evento;
- Identidade do sujeito que causou o evento;
- Categoria do evento;
- Descrição do evento.

5.4.2 Frequência de Processamento de Registos

Os registos devem ser analisados e revistos de modo regular, e adicionalmente sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. As ações tomadas baseadas na informação dos registos são também documentadas.

5.4.3 Período de Retenção de Registos de Auditoria

Os registos são mantidos disponíveis durante pelo menos 2 meses após processamento, e depois arquivados nos termos previstos na secção 5.5.

5.4.4 Proteção de Registos de Auditoria

Os registos são apenas analisados por elementos autorizados pertencentes aos Grupos de Trabalho.

Os registos são protegidos por mecanismos eletrónicos auditáveis de modo a detetar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

5.4.5 Procedimentos de Cópia de Segurança de Registos de Auditoria

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.4.6 Sistema de Recolha de Registos (Interno vs. Externo)

Os registos são recolhidos em simultâneo, interna e externamente aos sistemas das EC`s.

5.4.7 Notificação de Agentes Causadores de Eventos

Os eventos auditáveis são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

5.4.8 Avaliações de Vulnerabilidades

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebre de segurança do sistema.

5.5 Arquivo de Registos

5.5.1 Tipos de Registos Arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como a informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

5.5.2 Período de Retenção em Arquivo

Os dados sujeitos a arquivo são retidos por um período de 7 anos após a data de expiração do certificado a que digam respeito.

5.5.3 Proteção do Arquivo

O arquivo:

- É protegido para que apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao seu conteúdo;
- É protegido contra qualquer modificação ou tentativa de remoção;
- É protegido contra a deterioração do *media* onde é guardado, através de migração periódica para *media* novo;
- É protegido contra a obsolescência do hardware, sistemas operativos e outro software, pela conservação do hardware, sistemas operativos e outro software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal; e
- É guardado de modo seguro em ambientes externos.

5.5.4 Procedimentos para Cópia de Segurança do Arquivo

São efetuadas cópias de segurança dos arquivos, de modo incremental ou total e guardadas em dispositivos apropriados.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.5.5 Requisitos para Validação Cronológica de Registos

Algumas entradas dos arquivos contêm informação de data e hora baseadas em fonte de tempo segura.

5.5.6 Sistema de Recolha de Arquivo (Interno ou Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos para Obter e Verificar Informação de Arquivo

Apenas membros autorizados dos Grupos de trabalho têm acesso aos arquivos, sendo a sua integridade verificada através do seu restauro.

5.6 Renovação de Chaves

Sem Estipulação.

5.7 Recuperação em Caso de Desastre ou Comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1 Procedimentos em Caso de Incidente ou Desastre

As cópias de segurança das chaves privadas das EC`s (geradas e mentidas de acordo com a secção 6.2.4) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

5.7.2 Recursos Computacionais, Software e/ou Dados Corrompidos

No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, podem ser obtidas as cópias de segurança das chaves privadas da EC e os registos arquivados, para verificação da integridade dos dados originais.

Se for confirmado que os recursos computacionais, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a EC Multicert suspenderá os seus serviços e notificará a Entidade Supervisora.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

5.7.3 Procedimentos em caso de Comprometimento de Chave Privada da Entidade

No caso de a chave privada da EC Multicert ser comprometida ou haver suspeita de comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

- Notificação da Entidade Supervisora e todos os Titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC afetada;
- Revogação dos certificados emitidos no "ramo" da respetiva hierarquia de confiança e do certificado da EC afetada;
- Geração de novo par de chaves para a EC afetada;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC afetada.

5.7.4 Capacidades de Continuidade de Negócio em caso de Desastre

Os recursos computacionais, software, cópias de segurança e registos da EC devem ser arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após um desastre natural ou outro.

5.8 Cessação da EC ou ER

Em caso de cessação de atividade como prestador de serviços de confiança, a EC Multicert deve, atempadamente com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar a Entidade Supervisora;
b) Informar os Subscritores/Titulares de certificados;
c) Revogar todos os certificados emitidos;
d) Efetuar uma notificação final aos Subscritores/Titulares 2 dias antes da cessação formal da atividade;
e) Destruir ou prevenir a utilização, de forma definitiva, das chaves privadas;
f) Garantir a transferência para retenção de toda a informação relacionada com as atividades das EC`s, nomeadamente a chave da EC, certificados, disponibilidade de CRL`s, documentação armazenada (internamente ou externamente), repositórios e armazenamento de registos de eventos dentro do período definido na secção 5.5.2.

Em caso de alterações do organismo/estrutura responsável pela gestão da atividade da EC, a Multicert deve informar de tal facto às entidades listadas nas alíneas anteriores.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

6 Controlos de Segurança Técnica

Esta secção define as medidas de segurança implementadas pela EC Multicert de forma a proteger as chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras, assim como dados de ativação, estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Geração e Instalação do Par de Chaves

A geração dos pares de chaves das EC`s são processados de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do Par de Chaves

A geração de chaves criptográficas é feita pelos Grupos de Trabalho, compostos por elementos autorizados para tal, numa cerimónia planeadas e auditada de acordo com os procedimentos escritos para as operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos nos Grupos de Trabalho.

O hardware criptográfico usado para a geração de chaves da EC Multicert cumpre com os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+, e efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perda de dados, possa haver uma recuperação total e segura das chaves.

As chaves privadas para os certificados qualificados emitidos para pessoa singular ou coletiva (quando não são geradas pelo Subscritor/Titular em módulo seguro) são geradas pela EC através da utilização de hardware criptográfico que cumpre com os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+.

6.1.2 Entrega da Chave Privada ao Subscritor/Titular

No caso de o par de chaves ser gerado pela EC, a entrega da chave privada associada ao certificado para pessoa singular ou coletiva é efetuadas em dispositivo criptográfico SSCD (*Secure Signature-Creation Device*).

Para os restantes tipos de certificados, quando não é requerido que a chave privada esteja em QSCD, a chave privada é fornecida pelo Subscritor.

6.1.3 Entrega da Chave Pública ao Emissor do Certificado

A chave pública é entregue à EC, de acordo com os procedimentos indicados na secção 4.1.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

6.1.4 Entrega da Chave Pública da EC às *Relying Parties*

A chave privada da EC deve ser disponibilizada através do respetivo certificado, conforme a secção 2.2.

6.1.5 Tamanhos de Chave

O tamanho dos pares de chaves deve ser suficiente de forma a prevenir possíveis ataques de criptoanálise que descubram a chave privada correspondente ao par de chaves durante o seu período de utilização. Os tamanhos de chave estão definidos na secção 6.1.5 da DPC.

No caso das chaves RSA, o tamanho do módulo em bits tem que ser igualmente divisível por 8.

6.1.6 Geração dos Parâmetros de Chave Pública e Verificação de Qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo.

As chaves das EC`s são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#11.

6.1.7 Finalidades de Utilização da Chave (de acordo com o campo *key usage* X.509 v3)

De acordo com a secção 1.4 da DPC e documento Lista de Perfis de Certificados disponível em https://pki.multicert.com.

6.2 Proteção de Chave Privada e Controlos de Engenharia de Módulo Criptográfico

Nesta secção são considerados os requisitos para proteção das chaves privadas e para os módulos criptográficos da EC Multicert. A Multicert implementou uma combinação de controlos físicos, lógicos e procedimentais, devidamente documentados, de forma a assegurar a confidencialidade e integridade das suas chaves privadas.

6.2.1 Controlos e *Standards* de Módulo Criptográfico

Para a geração dos pares de chaves da EC Multicert, assim como para o armazenamento das chaves privadas, a Multicert utiliza um módulo criptográfico em hardware, que está em conformidades com os standards descritos na secção 6.2.1 da DPC.

6.2.2 Controlo Multi-Pessoal (n de m) da Chave Privada

O control multi-pessoal apenas é utilizado para as chaves da EC, dado que a chave privada dos certificados está sob controlo exclusivo do seu subscritor.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

A Multicert implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros de Grupos de Trabalho para efetuar operações criptográficas sensíveis na EC. Os dados de ativação necessários para a utilização das chaves privadas da EC Multicert são divididos em várias partes (guardadas nas chaves PED – pequenos tokens de identificação digital, com formato de caneta USB, identificando diferentes papéis no acesso ao HSM), acessíveis e à responsabilidade de diferentes membros dos Grupos de Trabalho. É necessário um determinado número destas partes (n) do total do número de partes (m) para ativar a chave privada da EC Multicert guardada no módulo criptográfico em hardware. São necessárias duas partes (n) para ativação da chave privada da EC.

6.2.3 Custódia de Chave Privada

As chaves privadas das EC`s geridas pela Multicert são armazenadas em token de hardware seguro, sendo feita uma cópia de segurança usando uma conexão direta de hardware para hardware entre os dois tokens seguros. A geração da cópia de segurança é o último passo quando é emitido um novo par de chaves para uma EC gerida pela Multicert.

O processo de cópia de segurança utiliza um HSM com duplo factor de autenticação (consola de autenticação portátil e chaves PED – pequenos tokens de identificação digitais, com a forma de caneta USB – que identificam diferentes papéis quando é feito o acesso ao HSM), em que diferentes pessoas, cada uma detendo uma chave PED, se devem autenticar antes que seja possível efetuar a cópia de segurança.

O token de hardware seguro com a cópia de segurança da chave privada da EC gerida pela Multicert é colocado num cofre localizado em instalações secundárias seguras e acessíveis apenas aos membros dos Grupos de Trabalho autorizados. O controlo de acesso físico a essas instalações previne o acesso não autorizado às chaves privadas.

A cópia de segurança da chave privada da EC gerida pela Multicert pode ser recuperada em caso de mau funcionamento da chave original. O processo de recuperação da chave utiliza os mesmos mecanismos de duplo factor de autenticação e com diferentes elementos, da mesma forma que é feito o processo de criação da cópia de segurança.

6.2.4 Cópia de Segurança da Chave Privada

A chave privada da EC tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme a secção 4.12 da DPC.

6.2.5 Arquivo de Chave Privada

As chaves privadas das EC`s, sujeitas a cópias de segurança, são arquivadas conforme identificado na secção 4.12 da DPC.

6.2.6 Transferência da Chave Privada para/de um Módulo Criptográfico

As chaves privadas da EC Multicert não são exportáveis a partir do token criptográfico FIPS 140-2 nível 3.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Mesmo que seja feita uma cópia de segurança das chaves privadas da EC Multicert para um outro token criptográfico, a cópia é feita diretamente, hardware para hardware, de forma a garantir o transporte das chaves entre módulos numa transmissão cifrada.

6.2.7 Armazenamento da Chave Privada em Módulo Criptográfico

As chaves privadas da EC Multicert são armazenadas de forma cifrada em módulos de hardware criptográfico.

6.2.8 Método de Ativação da Chave Privada

Para ativar as chaves privadas da EC é necessário, no mínimo, a intervenção de quatro elementos dos Grupos de Trabalho. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9 Método de Desativação da Chave Privada

A chave privada da EC é desativada quando o respetivo sistema é desligado.

Para desativar as chaves privadas das EC`s é necessário, no mínimo, a intervenção de quatro elementos dos Grupos de Trabalho. Uma vez desativada, esta permanece inativa até que o processo de ativação seja executado.

6.2.10 Método de Destruição da Chave Privada

As chaves privadas da EC (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado, assim que terminada a sua data de validade (ou se revogadas antes deste período).

A EC destrói as chaves privadas garantindo que não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza a função de formatação (inicialização a zeros) disponibilizada pelo hardware criptográfico ou outros meios apropriados, de forma a garantir a total destruição das chaves privadas das EC`s.

6.2.11 Avaliação/Nível do Módulo Criptográfico

Descrito na secção 6.2.1.

6.3 Outros Aspetos da Gestão do Par de Chaves

6.3.1 Arquivo da Chave Pública

É efetuada uma cópia de segurança das chaves públicas da EC Multicert pelos membros dos Grupos de Trabalho, permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante o seu prazo de validade.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

6.3.2 Períodos Operacionais do Certificado e Períodos de Utilização do Par de Chaves

O período de utilização das chaves pode ser o mesmo que o período de validade do certificado.

Os certificados assinados por uma EC específica têm que expirar antes do período de validade do par de chaves da EC.
A validade dos vários tipos de certificados está descrita na secção 6.3.2 da DPC.

6.4 Dados de Ativação

6.4.1 Geração e Instalação de Dados de Ativação

Os dados de ativação necessários para a utilização das chaves privadas da EC são divididos em várias partes (guardadas em chaves PED – pequenos tokens de identificação digital, com o formato de caneta USB – que identificam diferentes papéis no acesso ao HSM), ficando à responsabilidade de diferentes membros dos Grupos de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves, e obedecem aos requisitos definidos pelo *standard* FIPS 140-2 nível 3.

6.4.2 Proteção de Dados de Ativação

Os dados de ativação (em partes separadas e/ou palavra-passe) são memorizados e/ou armazenados em tokens que evidenciem tentativas de violação e/ou guardados em envelopes que são armazenados em cofres seguros.

As chaves privadas da EC são guardadas, de forma cifrada, em token criptográfico.

6.4.3 Outros Aspetos dos Dados de Ativação

Se for necessário transmitir os dados de ativação das chaves privadas, esta transmissão será protegida contra perdas de informação, roubo, alteração de dados e divulgação não autorizada.

Os dados de ativação são destruídos (por formatação e/ou destruição física) quando a chave privada associada é destruída.

6.5 Controlos de Segurança Computacional

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

O acesso aos servidores da EC Multicert é restrito aos membros dos Grupos de Trabalho com um motivo válido para esse acesso. A EC Multicert funciona online, sendo o pedido de emissão de certificado efetuado a partir do Sistema de Gestão do Ciclo de Vida dos Certificados (SGCVC) e/ou da consola de operação.

A EC Multicert e o SGCVC dispõem de dispositivos de proteção de fronteira, nomeadamente sistema firewall, e estão em conformidade com os requisitos necessários para identificação,

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

autenticação, controlo de acessos, administração, auditoria, reutilização, responsabilidade e recuperação de serviços, e troca de informação.

6.5.2 Avaliação/Nível de Segurança Computacional

Os vários sistemas e produtos utilizados pela EC são fiáveis e protegidos contra modificações.

O módulo criptográfico em Hardware da EC está em conformidade com o standard EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

6.6 Controlos Técnicos do Ciclo de Vida

6.6.1 Controlos de Desenvolvimento de Sistema

As aplicações são desenvolvidas e implementadas de acordo com as regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecida metodologia auditável que permite verificar que o software da EC Multicert não fi alterado antes da sua primeira utilização. Todas as configurações e alterações do software são executadas e auditadas por membros dos Grupos de Trabalho.

6.6.2 Controlos de Gestão da Segurança

A Multicert tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas das EC`s. Quando utilizado pela primeira vez, o sistema da EC Multicert é verificado para garantir que o software utilizado é fidedigno, legal e que não foi alterado depois da sua instalação.

6.6.3 Controlos de Segurança do Ciclo de Vida

As operações de atualização e manutenção dos produtos e sistemas da EC Multicert seguem o mesmo controlo que o equipamento original e são instalados pelos membros dos Grupos de Trabalho com formação adequada para o efeito, seguindo os procedimentos definidos.

6.7 Controlos de Segurança da Rede

As EC`s dispõem de dispositivos de proteção de fronteira, nomeadamente sistema firewall, e cumprem com os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditoria, reutilização, responsabilidade e recuperação de serviços, e troca de informação.

6.8 Validação Cronológica

Os certificados, CRL`s e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Todas estas entradas são assinadas digitalmente por um certificado emitido para o efeito.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

7 Perfis de Certificado, CRL e OCSP

7.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo subscritor (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através da utilização de certificados digitais X.509 v3, que são a estrutura de dados que faz a ligação entre a chave pública e o seu Subscritor. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo Subscritor.

Um certificado tem um período de validade limitado, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC, e zero ou mais certificados adicionais de EC`s assinados por outras EC`s.

O perfil de certificado de servidor web está em conformidade com:

- ITU.T recommendationX.509[2];
- RFC 5280[3];
- Legislação aplicável, nacional e europeia; e
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

Os perfis de certificados podem ser consultados no documento Lista de Perfis de Certificados disponível em https://pki.multicert.com.

7.1.1 Número(s) de Versão

O campo “*version*” do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é a versão 3 do X.509.

[2] cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

[3] cf. RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

7.1.2 Extensões dos Certificados

As extensões dos certificados emitidos pela PKI Multicert estão em conformidade com o RFC 5280.

7.1.3 Identificadores de Objeto de Algoritmo

Os certificados emitidos pela PKI Multicert são assinados usando o algoritmo sha256WithRSAEncryption (1.2.840.113549.1.1.11):

{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

7.1.4 Formatos de Nome

De acordo com o definido na secção 3.1.

7.1.5 Restrições de Nome

A Multicert pode incluir restrições de nome no campo nameConstraints, quando aplicável.

7.1.6 Identificador de Objeto de Política de Certificado

Todos os certificados emitidos pela PKI Multicert contêm os seguintes qualificadores:

"*policyQualiflierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*", que aponta para o URI onde se encontra a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". São incluídos outros identificadores de objetos de política de certificado, dependendo do tipo de certificado, de acordo com a secção 1.2 deste documento, e de acordo com o descrito no documento Lista de Perfis de Certificados (MULTICERT_PJ.ECRAIZ_428_pt) disponível em https://www.pki.multicert.com.

7.1.7 Utilização de Extensão de Restrições de Política

Sem Estipulação.

7.1.8 Sintaxe e Semânticas de Qualificadores de Política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores de certificados e autores da política de certificado. O tipo de qualificador é o "*CPSuri*", que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC, e o "*userNotice explicitText*", que contém um apontador, na forma de URI, para a Política de Certificado.

7.1.9 Processamento de Semânticas para a Extensão de Políticas de Certificado Críticas

Sem Estipulação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

7.2 Perfil de CRL

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, existem várias circunstâncias que podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o sujeito e os dados do certificado (por exemplo, um trabalhador que termina o emprego), o comprometimento ou suspeita de comprometimento da correspondente chave privada. Nestas circunstâncias, quando a EC tem conhecimento revoga o certificado[3].

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC ou CRL). A CRL é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na CRL pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a CRL mais recente e verificar se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova CRL periodicamente[3].

O perfil de CRL está em conformidade com:

- ITU.T Recommendation X.509[2];
- RFC 5280[3]; e
- Legislação aplicável, nacional e europeia.

7.2.1 Número(s) de Versão

As EC`s emitem CRL`s em conformidade com a versão 2 do RFC 5280.

7.2.2 CRL e Extensões da CRL

As EC`s emitem extensões da CRL de acordo com o RFC 5280.

7.3 Perfil OCSP

O perfil de certificados OCSP está em conformidade com:

- ITU.T recommendation X.509[2];
- RFC 6960[4]; e
- Legislação aplicável, nacional e europeia.

7.3.1 Número(s) de Versão

As EC`s suportam a versão 1 do RFC 6960.

[4] cf. RFC 6960. 2013, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

7.3.2 Extensões OCSP

Sem Estipulação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

8 Auditoria de Conformidade e Outras Avaliações

São realizadas auditorias internas a esta PC e a outras regras, procedimentos, cerimónias e processos.

A PKI Multicert é sujeita a auditorias externas, realizadas por uma Entidade de Avaliação de Conformidade (CAB), de forma a avaliar a conformidade da PKI Multicert e ER`s relativamente à legislação Nacional e Europeia aplicável.

8.1 Frequência ou Circunstâncias da Avaliação

As auditorias de conformidade são realizadas anualmente. A Multicert necessita provar, através dos relatórios de auditoria (produzidos por uma Entidade de Avaliação de Conformidade), que está em conformidade com a legislação Nacional e Europeia aplicável.

8.2 Identificação/Qualificações do Avaliador

As auditorias externas de conformidade são realizadas por uma Entidade de Avaliação de Conformidade (CAB) devidamente acreditada[5].

O Organismo Nacional de Acreditação (NAB) é responsável pela credenciação das Entidades de Avaliação da Conformidade (CAB) com base na EN ISO/IEC 17065 conforme perfil da ETSI EN 319 403, estando estes capacitados a efetuar as avaliações de conformidade resultando dessas avaliações um Relatório de Conformidade (CAR) a ser disponibilizado à Entidade Supervisora e outras partes interessadas, para avaliar a continuidade da disponibilização de serviços de confiança.

8.3 Relação do Avaliador com a Entidade Avaliada

O auditor e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na relação entre o auditor e a entidade submetida a auditoria, deve ser garantida inexistência de qualquer vínculo contratual, financeiro, dependência legal ou organizacional, ou qualquer outra dependência que possa gerar conflito de interesses.

8.4 Tópicos Abrangidos pela Avaliação

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação Nacional e Europeia aplicável e com esta PC e outras regras, procedimentos e processos (especialmente

[5] https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação, e gestão do ciclo de vida dos certificados).

8.5 Ações Tomadas como Resultado de Deficiências

Se de uma auditoria resultarem não conformidades, o auditor procede da seguinte forma:

a) Documenta todas as não conformidades encontradas durante a auditoria no Relatório de Avaliação de Conformidade (CAR). Dependendo da severidade das não conformidades:
    a. Falha se as não conformidades forem severas, neste caso o serviço de confiança auditado não é certificado em conformidade;
    b. Passa se as não conformidades não forem severas, neste caso o serviço de confiança auditado tem 3 meses para corrigir as não conformidades, desempenhando os passos abaixo.
b) Tendo em conta as não conformidades constantes no CAR, a entidade submetida à auditoria enviará um Plano de Ações Corretivas, no qual devem estar descritas as ações, metodologia e tempo necessário para corrigir as não conformidades;
c) O CAB, depois de analisar este plano de ações toma umas das seguintes opções:
    a. Aceita as ações propostas, neste caso após as ações estarem implementadas é realizada uma auditoria de verificação para validar a eficácia da implementação das ações;
    b. Não aceita as ações propostas, neste caso o auditado tem que propor outro plano de ações.

8.6 Comunicação de Resultados

Os resultados devem ser sempre comunicados à Entidade Supervisora e outras partes interessadas.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9 Outras Matérias Legais e de Negócio

9.1 Taxas

9.1.1 Taxas de Emissão ou Renovação de Certificado

As taxas cobradas pela Multicert estão identificadas na sua loja online ou numa proposta formal realizada pela Multicert.

9.1.2 Taxas de Acesso a Certificado

Sem Estipulação.

9.1.3 Taxas de Acesso a Informação de Estado ou Revogação

O acesso a informação sobre o estado de certificado ou revogação (CRL e Delta CRL) é gratuita e livre.

9.1.4 Taxas para Outros Serviços

As taxas para a validação cronológica e OCSP on-line são identificadas numa proposta formal realizada pela Multicert.

9.1.5 Política de Reembolso

Sem Estipulação.

9.2 Responsabilidade Financeira

9.2.1 Cobertura de Seguro

A Multicert dispõe do seguro obrigatório de responsabilidade civil, conforme o artigo 20.º do Decreto-Lei n.º 12/2021, e Portaria nº 62/2021.

9.2.2 Outros Recursos

Sem Estipulação.

9.2.3 Cobertura de Seguro ou Garantia para Utilizadores Finais

A Multicert dispõe do seguro obrigatório de responsabilidade civil, conforme o artigo 20.º do Decreto-Lei n.º 12/2021, e Portaria n.º 62/2021.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.3 Confidencialidade de Informação de Negócio

9.3.1 Âmbito de Informação Confidencial

Declara-se expressamente como informação confidencial, aquela que não poderá ser divulgada a terceiros, nomeadamente:

- As chaves privadas das EC`s da PKI;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal fornecida à EC durante o processo de registo dos Subscritores de certificados, salvo se houver autorização explícita para a sua divulgação e/ou se a mesma não for incluída no conteúdo do certificado emitido;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Informação de todos os documentos relacionados com a PKI Multicert (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade da Multicert. Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho da PKI Multicert com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita da Multicert;
- Todas as palavras-chave, PIN`s e outros elementos de segurança relacionados com as EC`s da PKI Multicert;
- A identificação dos membros dos Grupos de Trabalho da PKI Multicert;
- A localização dos ambientes da PKI Multicert e seu conteúdo.

9.3.2 Informação fora do Âmbito de Informação Confidencial

É considerada informação de acesso público:

- Política de Certificado;
- Declaração de Práticas de Certificação;
- CRL;
- Delta CRL;
- Toda a informação classificada como “Público” (a informação que não esteja expressamente considerada “pública” deve ser considerada confidencial).

A EC permite o acesso a informação não confidencial sem prejuízo dos controlos de segurança necessários para proteger a autenticidades e integridade da informação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.3.3 Responsabilidade de Proteção de Informação Confidencial

Os elementos dos Grupos de trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito da Multicert.

9.4 Privacidade de Informação Pessoal

9.4.1 Plano de Privacidade

A EC é responsável por implementar as medidas que assegurem a privacidade dos dados pessoais, de acordo com a legislação Portuguesa e Europeia.

9.4.2 Informação Tratada como Privada

É considerada informação privada toda a informação fornecida pelo Subscritor/Titular do certificado que não seja disponibilizada no certificado digital do Subscritor/Titular ou CRL.

9.4.3 Informação Não Considerada Privada

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo Subscritor/Titular do certificado que seja disponibilizada no certificado digital do Subscritor/Titular ou CRL.

9.4.4 Responsabilidade pela Proteção de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

9.4.5 Notificação e Consentimento para Utilização de Informação Privada

De acordo com a legislação Portuguesa e Europeia aplicável.

9.4.6 Divulgação Resultante de Processo Judicial ou Administrativo

Sem Estipulação.

9.4.7 Outras Circunstâncias de Divulgação de Informação

Sem Estipulação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.5 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, CRL, Delta CRL emitidos, OID, DPC e PC, bem como qualquer outro documento relativo à PKI Multicert, pertencem à Multicert S.A..

As chaves privadas e as chaves públicas são propriedade do Subscritor/Titular, independentemente do meio físico que se utilize para o seu armazenamento.
O Subscritor/Titular reserva sempre o direito sobre as marcas, produtos ou nome comercial contido no certificado.

9.6 Representações e Garantias

9.6.1 Representações e Garantias da EC

As EC`s são obrigadas a:

a) Desempenhar as suas operações de acordo com esta política;
b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;
c) Proteger as suas chaves privadas;
d) Emitir certificados de acordo com o *standard* X.509;
e) Emitir certificados que estejam conformes com a informação conhecida no momento da sua emissão e livres de erros de entrada de dados;
f) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao Subscritor/Titular através de um procedimento seguro;
g) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e garantam a segurança técnica e criptográfica dos processos de certificação;
h) Utilização sistemas confiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir a modificação de dados por pessoas não autorizadas;
i) Arquivar os certificados emitidos sem quaisquer alterações;
j) Garantir que podem determinar com precisão a data e hora em que o um certificado foi emitido, revogado ou suspenso;
k) Empregar pessoal com qualificações, conhecimento e experiência necessária para a prestação de serviços de certificação;
l) Revogar os certificados nos termos da secção 4.9 deste documento, e publicar os certificados revogados no repositório da CRL das EC Multicert, com a frequência estabelecida na secção 4.9.7;
m) Publicar no seu repositório a DPC e Políticas de Certificado garantindo o acesso às versões atuais;
n) Disponibilizar as versões anteriores da DPC;
o) Notificar com a rapidez necessária, por email, os subscritores de certificado caso uma EC revogue ou suspenda o certificado, indicando a razão correspondente para tal ação;
p) Colaborar com as auditorias realizadas pela Entidade de Avaliação de Conformidade;

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

q) Operar de acordo com a legislação aplicável;
r) Proteger eventuais chaves existentes que estejam sob a sua custódia;
s) Garantir a disponibilidade da CRL de acordo com o disposto na secção 2;
t) Comunicar com uma antecedência mínima de 2 meses a todos os Titulares dos certificados emitidos assim como à Entidade Supervisora, em caso de cessar a sua atividade;
u) Cumprir com as especificações contidas no regulamento Europeu e legislação Portuguesa sobre a Proteção de Dados Pessoais;
v) Manter toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento, durante 7 (sete) anos após a expiração do certificado;
w) Disponibilizar os certificados das EC`s.

9.6.2 Representações e Garantias da ER

As Entidades de Registo são obrigadas a:

a) Desempenhar as suas operações de acordo com esta política;
b) Permitir a emissão de certificados livres de erros de entrada de dados;
c) Garantir a confidencialidade no processo de geração dos dados de criação da assinatura e na sua entrega ao Subscritor/Titular através de um procedimento seguro;
d) Utilizar sistemas e produtos confiáveis que estejam protegidos contra todas as modificações e garantam a segurança técnica e criptográfica dos processos de certificação;
e) Arquivar os certificados emitidos sem quaisquer alterações;
f) Empregar pessoal com as qualificações, conhecimento e experiência necessária para a prestação de serviços de confiança;
g) Colaborar com as auditorias realizadas pela Entidade de Avaliação de Conformidade;
h) Operar de acordo com a legislação aplicável, nomeadamente de acordo com o Regulamento 910/2014;
i) Proteger eventuais chaves existentes que estejam sob sua custódia;
j) Comunicar com uma antecedência mínima de dois meses a todos os Titulares dos certificados emitidos assim como à Entidade Supervisora, em caso de cessar a sua atividade;
k) Cumprir com as especificações contidas no regulamento Europeu e sobre Proteção de Dados Pessoais;
l) Manter toda a informação e documentação relativa a um certificado reconhecido em cada momento, durante 7 anos após a expiração do certificado.

9.6.3 Representações e Garantias do Subscritor/Titular

É obrigação do Subscritor/Titular do certificado emitido:

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

a) Limitar e ajustar a utilização do certificado de acordo com as finalidades previstas na Política de Certificado, Condições Gerais de Emissão de Certificado Digital, e secção 1.4 da DPC;
b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita do comprometimento da chave privada correspondente à chave pública contida no certificado, ou outra razão constante na secção 4.9;
d) Não utilizar o certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspenso ou expirado o seu período de validade;
e) Submeter à Entidade de Certificação (ou Entidade de Registo) a informação que considere exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação; e
f) Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implementação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da Multicert S.A..

9.6.4 Representações e Garantias das *Relying Party*

É obrigação das partes que confiem nos certificados emitidos pela EC:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na correspondente Política de Certificado e secção 1.4 da DPC;
b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
c) Assumir a responsabilidade pela correta verificação das assinaturas digitais;
d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados nos quais confia;
e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia, e aceitar sujeitar-se às mesmas;
f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como razão para revogação do mesmo, utilizando os meios que a Multicert indique na sua DPC.

9.6.5 Representações e Garantias de outros Participantes

Sem Estipulação.

9.7 Renúncia de Garantias

A Multicert recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta PC.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.8 Limitações de Responsabilidade

A Multicert S.A., enquanto Entidade de Certificação:

a) Responde pelos atos e omissões no exercício da sua atividade de acordo com o Artigo 15º do Decreto-lei 12/2021;

b) Responde pelos prejuízos que cause aos Subscritores/Titulares ou a terceiros pela falta ou atraso na inclusão de um certificado revogado ou suspenso no serviço de consulta de validade dos certificados, uma vez que tenha conhecimento dele;

c) Assume toda a responsabilidade mediante terceiros pelas funções necessárias à prestação de serviços de confiança, no âmbito da atuação dos Subscritores/Titulares;

d) A sua responsabilidade de administração / gestão assenta numa base objetiva e abrange todo o risco que os particulares sofram sempre que este seja consequência do funcionamento normal ou anormal dos seus serviços;

e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando os limites da utilização possível não tenham sido consignados no certificado, de forma clara reconhecida por terceiros;

f) Não responde quando o Subscritor/Titular supera os limites que constam no certificado quanto às suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao Subscritor/Titular;

g) Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que constam no certificado quanto às suas possíveis utilizações;

h) Não assume qualquer responsabilidade no caso de perda ou prejuízo:

   i. Dos serviços prestados, em caso de guerra, desastre natural ou qualquer outro motivo de força maior;

   ii. Resultante da utilização dos certificados quando esta utilização exceda os limites estabelecidos na DPC e PC;

i) Resultante do uso indevido ou fraudulento dos certificados ou CRL`s emitidas pelas EC`s da PKI Multicert.

   i)

9.9 Indemnizações

De acordo com a legislação em vigor.

9.10 Prazo e Terminação

9.10.1 Prazo

Os documentos relacionados com a EC Multicert (incluindo esta PC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão.

Esta PC entra em vigor desde o momento da sua publicação no repositório da EC Multicert.

Esta PC mantém-se em vigor enquanto não for revogada expressamente pela emissão de uma nova versão.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.10.2 Terminação

As alterações são adequadamente registadas com indicação de uma versão menor.

As alterações tornam-se efetivas após a aprovação do Grupo de Trabalho de Gestão e a publicação no repositório de uma nova versão maior.

9.10.3 Efeito da Terminação e Sobrevivência

As obrigações e restrições estabelecidas nesta PC, relativamente a auditorias, informação confidencial, arquivo de registos, obrigações e responsabilidades, criadas sob a sua vigência, subsistirão após a sua substituição por uma nova versão em tudo o que não se oponha a esta.

9.11 Notificações Individuais e Comunicações aos Participantes

Qualquer notificação relacionada com esta PC deve ser feita por correio eletrónico assinado digitalmente, formulários assinados enviados por correio, ou outros, dependendo da criticidade e assunto da comunicação. Estas notificações devem ser enviadas para os contactos indicados na secção 1.5.

9.12 Alterações

9.12.1 Procedimento para Alteração

As alterações a esta PC são realizadas pelo Grupo de Trabalho de Autenticação. Podem ser submetidas ao Grupo de Trabalho de Autenticação sugestões de alterações para serem analisadas, através dos contactos fornecidos na secção 1.5.

O Grupo de Trabalho de Autenticação regista as alterações da revisão em versões menores na PC. Quando se encontra pronta para aprovação uma nova versão da PC, o Grupo de Trabalho de Autenticação submete o documento para aprovação pelo Grupo de Trabalho de Gestão, sendo incrementada uma versão maior à PC.

9.12.2 Mecanismo e Período de Notificação

As alterações à PC são registadas na tabela Histórico de Versões, contendo identificação da versão, data, e detalhes das alterações feitas.

Quando é aprovada uma nova versão maior da PC pelo Grupo de Trabalho de Gestão, é publicada no repositório da Multicert uma versão atualizada deste documento.

9.12.3 Circunstâncias nas quais o OID deve ser Alterado

Se o Grupo de Trabalho de Autenticação determinar que é necessário alterar o OID correspondente à DPC ou PC, propõe essa alteração ao Grupo de Trabalho de Gestão. Neste caso, é criado um novo documento DPC ou PC com um OID diferente.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

De outra forma, as alterações não devem requerer a alteração do OID da DPC ou PC.

9.13 Disposição de Resolução de Conflito

Em caso de litígio o consumidor pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A lista oficial de tais entidades está disponível no Portal do Consumidor em www.consumidor.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento quanto a qualquer conflito decorrente da interpretação, aplicação ou execução do presente formulário de emissão, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

9.14 Legislação Aplicável

A Multicert, enquanto entidade que presta serviços de confiança, tais como os serviços de certificação digital, é obrigada a cumprir os requisitos estabelecidos na atual legislação portuguesa e europeia.

Pode ser encontrada mais informação sobre a legislação e standards aplicáveis à PKI Multicert na secção 1.6.3.

9.15 Conformidade com a Legislação Aplicável

Ver secção 9.14.

9.16 Outras Disposições

9.16.1 Acordo Completo

Todas as *relying parties* assumem na totalidade o conteúdo da última versão desta PC.

9.16.2 Atribuição

As partes que operam sob esta PC ou acordos aplicáveis não podem atribuir os seus direitos ou obrigações sem o prévio consentimento por escrito da Multicert.

9.16.3 Divisibilidade

Se uma disposição desta PC, incluindo cláusulas de limitação de responsabilidade, for considerada ineficaz ou não executável, o restante desta PC deve ser interpretado no sentido da intenção original das partes. Qualquer disposição desta PC que estabeleça uma limitação de responsabilidade deve ser separável e independente de qualquer outra disposição e deve ser aplicada como tal.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

9.16.4 Execução (Honorários de Advogados e Renúncia de Direitos)

A Multicert pode requerer a indemnização e honorários de advogados de uma parte por danos, perdas e despesas relacionadas à conduto dessa parte. A falha da Multicert em aplicar uma cláusula desta PC não renuncia ao direito da Multicert de aplicar a mesma cláusula posteriormente ou ao direito de aplicar quaisquer outras cláusulas desta PC. Para ter efeito, qualquer renúncia deve ser feita por escrito e assinada pela Multicert.

9.16.5 Força Maior

As cláusulas de força maior estão incluídas nas Condições Gerais de Emissão de Certificado Digital.

9.17 Outras Provisões

Sem Estipulação.

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.

Aprovação

Nuno Ponte (Grupo de Trabalho de Gestão)

[Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte

Digitally signed by [Assinatura Qualificada] Nuno Miguel Arieiro Rodrigues da Ponte
Date: 2023.07.10 17:36:30 +01'00'

Copyright © 2002 -2023 MULTICERT - Todos os direitos reservados.